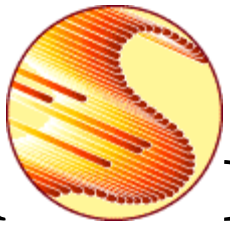


Sandstorm Enterprises

PhoneSweep® Gold

User Manual

For use with PhoneSweep® v4.0 and later versions.

Sandstorm Enterprises, Inc.
PO Box 381548
Cambridge, MA 02238-1548
http://www.sandstorm.net/
sales@sandstorm.net
support@sandstorm.net

Tel: 617-426-5056
Fax: 617-357-6042

June 19, 2002

[This Page Intentionally Blank]

Table of Contents

1 Introduction 6
2 A Tour Of PhoneSweep Gold 7
2.1 PhoneSweep Gold Icon Quick Reference Chart 8
3 Installation and Setup 10
3.1 System Requirements 10
3.1.1 Distributed Requirements 10
3.1.2 E-mail Notification Requirements 10
3.1.3 Merged Reporting 11
3.1.4 Security 11
3.1.5 Operating System 11
3.2 Using PhoneSweep Gold's Distributed feature over the Internet or Corporate LAN/WAN 12
3.2.1 Router (Access Lists) 12
3.2.2 VPN issues 12
3.2.3 Firewall issues 12
3.2.4 NAT issues 12
3.3 Upgrading Existing PhoneSweep 4.0 Copies to PhoneSweep Gold 13
3.4 Hardware License Protection and Gold 14
3.5 Troubleshooting Gold Issues 14
3.6 Uninstalling PhoneSweep Gold 14
3.7 Reinstalling PhoneSweep Gold 15
4 Setting Up Distributed Sweeps 16
4.1 Setting Up And Managing Distributed PhoneSweep 22
4.1.1 What does Distributed allow me to do? 22
4.1.2 PhoneSweep Distributed Access Control 23
4.1.3 Before Setting Up 24
4.1.4 Setting up 24
4.1.5 Managing Distributed Session Connections 25
4.1.6 Importing and Exporting with Remote Sessions 26
4.2 Possible Distributed PhoneSweep Injuries 26
5 Setting Up And Managing Automatic E-mail Notifications 28
5.1 Setting Up A Test E-mail Notification 29
5.1.1 Verify e-mail addresses and notify recipients prior to scanning. 30
5.1.2 Test sweep to verify e-mail notification addresses 30
5.2 Sample Gold E-mail Notification Message 30
5.3 Possible E-mail Notification Injuries 31
6 Generating Merged Reports 32
6.1 Possible Merged Report Injuries 34
Appendix A: PhoneSweep Gold FAQ 35
Distributed PhoneSweep 35
How is Distributed beneficial to me? 35
What are the advantages and disadvantages of choosing one access control level over another? 35
Why do I need someone local to perform a sweep at remote sites? 35
Why do I still need a Local Manager or someone with access to the PhoneSweep Gold Machine and PhoneSweep at each remote site? 36
Why does operation on my remote copy of PhoneSweep Gold seem so slow? 36

E-mail Notification 36
How is E-Mail Notification beneficial for my organization? 36
I am getting thousands of e-mail messages! How do I stop this from happening? .. 37
What is SMTP and how do I get the address for my SMTP server? 37
Merged Reports 37
What can Merged Reporting do for me? 37
Why is Merged Report Generation so slow? 37
Why are the percentages not what I expected in my Merged Report? 37
Is there Merged Charting? 37
Improving Distributed PhoneSweep's Performance 38
Improving E-mail Notification Performance 38
Improving Merged Reports Performance 39
Managing Multiple Connections Across Networks 39
Managing Remote Connections across an internal network or VPN-based WAN ... 39
Managing Remote Connections across the Internet 39
Internet Primer 40
Miscellaneous Questions 41
I want to set up PhoneSweep Gold's distributed feature in multiple countries. What do you recommend in terms of equipment? 41
Appendix B: PhoneSweep Gold Troubleshooting Guide 43
Common Problems and Possible Solutions 43
Distributed 43
Merged Reports 44
E-mail Notifications 44
PhoneSweep Gold Error and Warning Messages 45
Distributed messages 45
E-mail Notification messages 46
Merged Reporting messages 46
Appendix C: Sample PhoneSweep Merged Report 47
Executive Summary of PhoneSweep Scan 48
Engineering Summary of PhoneSweep Scan 49
Introduction: 49
PhoneSweep Terminology: 49
Call Response States: 50
Dialed Phone Numbers: 50
Discovered Fax Machines: 51
Discovered Modems: 51
Penetrated Modems: 51
Anomalies: 51
Systems Penetrated by PhoneSweep: 51
Carrier Numbers Found: 51
Busy Numbers Found: 52
Tone Numbers Found: 52
Fax Numbers Found: 52
Incomplete Scan Areas: 52
Identified Systems with Modems: 52
Unidentified Carrier Numbers: 53
Responses from Penetrated Systems: 53

Responses From Unknown Modems: 53
Appendix A: Responses from target modems 54
Appendix B: Phone Number Taxonomy 55
Appendix C: List of all calls and their results 57

1 Introduction

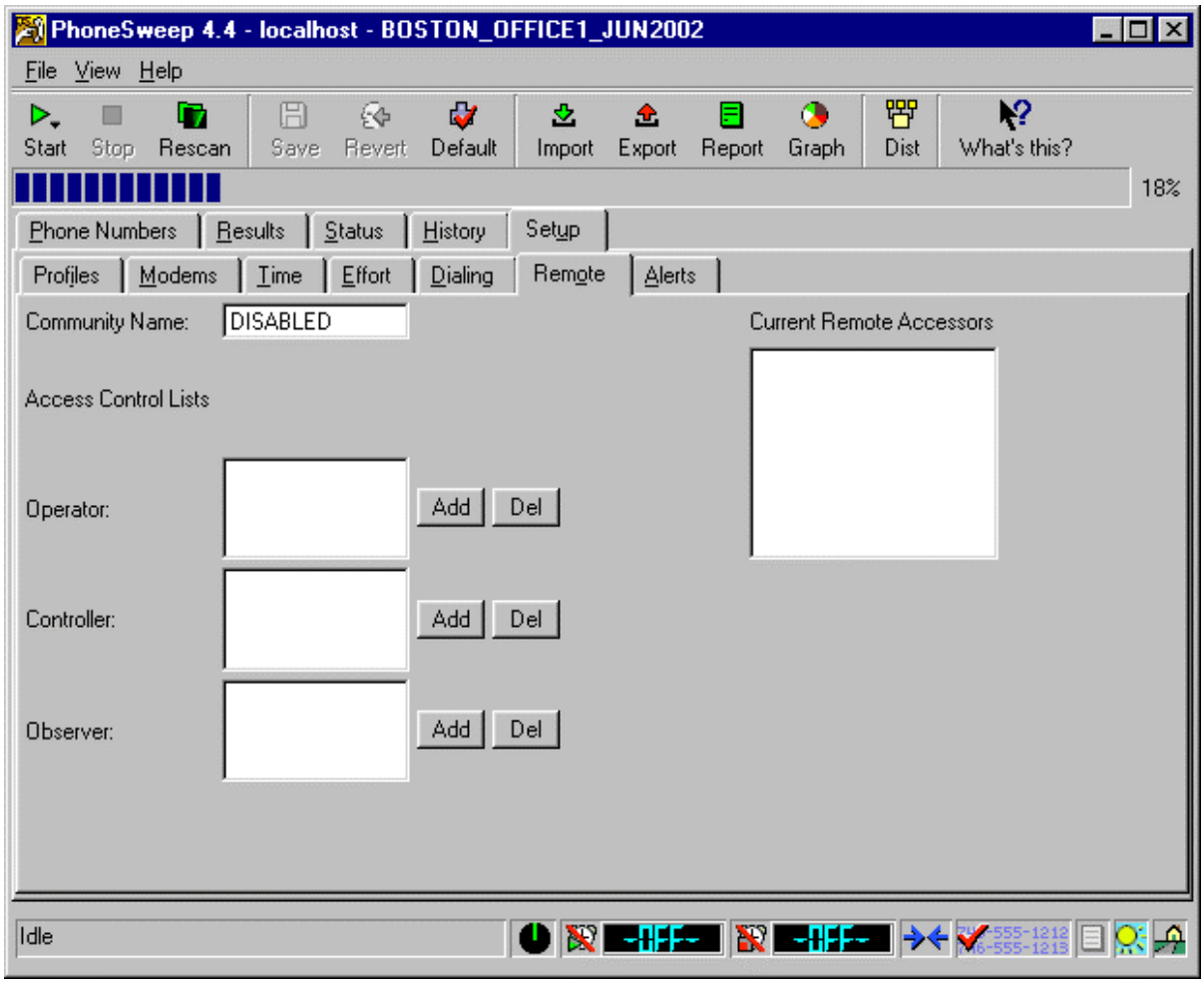
Welcome to PhoneSweep® Gold!

PhoneSweep Gold is an enhancement package for the PhoneSweep telephone system security audit tool. It adds high-end functionality to PhoneSweep that some users have requested as a critical need. By providing these functions as an optional add-on, we can continue evolving PhoneSweep's primary capabilities at the reasonable cost that customers have come to expect from us. If any of the following features meet a critical need, then PhoneSweep Gold is for you:

- **Automatic E-mail Notification:** Specify a set of events that, when they occur during a scan, will generate automatic e-mail notifications to one or more e-mail addresses. For example, if you want to know the instant a carrier is detected, PhoneSweep Gold can send e-mail to your pager to alert you.
- **Merged Reporting:** Generate a single report from multiple profiles. For example, this feature allows a company that currently has a separate scan for each department to create a report covering the entire company.
- **Distributed PhoneSweep (minimum of 2 copies of PhoneSweep with accompanying Gold additions required)**: Link multiple copies of PhoneSweep for remote operation from one or more sources. This feature enables companies that have many dispersed locales to centrally operate a scan, thus saving the company the expense of sending a person to each remote location. It also enables scans to be performed via many locally dialed numbers, rather than being subjected to long distance phone charges.

2 A Tour Of PhoneSweep Gold

PhoneSweep Gold seamlessly integrates with the main PhoneSweep user interface, adding buttons, menu options and sub-tabs without affecting other PhoneSweep functions. Integration is initiated by the PhoneSweep Gold dongle, so users need do nothing more than ensure that the correct dongle is attached to their system for Gold enhancements to be available.

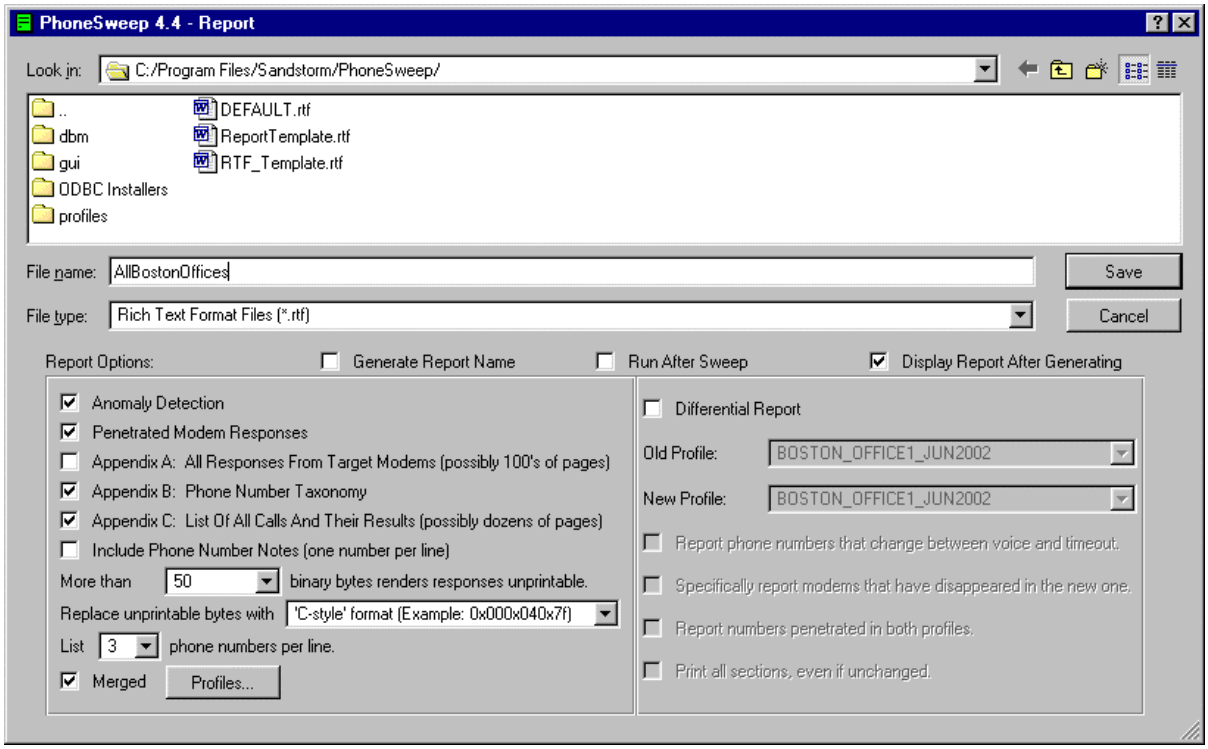

PhoneSweep 4.4 - localhost - BOSTON_OFFICE1_JUN2002
File View Help
Start Stop Rescan Save Revert Default Import Export Report Graph Dist What's this?
18%
Phone Numbers Results Status History Setup
Profiles Modems Time Effort Dialing Remote Alerts
Community Name: DISABLED
Current Remote Accessors
Access Control Lists
Operator: Add Del
Controller: Add Del
Observer: Add Del
Idle

PhoneSweep window with Gold options

Please take a moment to familiarize yourself with new Gold features as they appear on the PhoneSweep user interface:

- Gold adds two new sub-tabs under the **Setup** tab:
    - **Remote** (shown): Allows you to control who can use your copy of PhoneSweep remotely.
    - **Alerts** (to the right of Remote tab): Allows you to control e-mail notification.
- The **Dist** button (** **) along the top of the PhoneSweep user interface allows you to control PhoneSweep activities at remote locations and view remote connections.

- The **Merged Reports** feature is added to the **Reports** pop-up window. A **Merged** checkbox appears on the lower left hand side of the **Report** pop-up window, along with the **Profiles** button. Clicking on the **Profiles** button brings up a list of profiles, from which you can select the individual profiles you want to merge.


PhoneSweep 4.4 - Report
Look in: C:/Program Files/Sandstorm/PhoneSweep/
..
dbm
gui
ODBC Installers
profiles
DEFAULT.rtf
ReportTemplate.rtf
RTF_Template.rtf
File name: AllBostonOffices
Save
File type: Rich Text Format Files (*.rtf)
Cancel
Report Options:
Generate Report Name
Run After Sweep
Display Report After Generating
Anomaly Detection
Penetrated Modem Responses
Appendix A: All Responses From Target Modems (possibly 100's of pages)
Appendix B: Phone Number Taxonomy
Appendix C: List Of All Calls And Their Results (possibly dozens of pages)
Include Phone Number Notes (one number per line)
More than 50 binary bytes renders responses unprintable.
Replace unprintable bytes with 'C-style' format (Example: 0x000x040x7f)
List 3 phone numbers per line.
Merged
Profiles...
Differential Report
Old Profile: BOSTON_OFFICE1_JUN2002
New Profile: BOSTON_OFFICE1_JUN2002
Report phone numbers that change between voice and timeout.
Specifically report modems that have disappeared in the new one.
Report numbers penetrated in both profiles.
Print all sections, even if unchanged.

2.1 PhoneSweep Gold Icon Quick Reference Chart

The following icons appear in the PhoneSweep window when you add Gold. For a complete list of PhoneSweep icons, please refer to the *PhoneSweep Manual* under Section 2.2, "PhoneSweep Icon Quick Reference Chart."

PhoneSweep Gold Icons

	Distributed Connect
	Distributed Disconnect
	Distributed Get Profile from remote session
	Distributed Put Profile to remote session
	Distributed Icon (activate Distributed Overview)
	Current Active Session selected on Distributed Overview
	Distributed Switch Sessions
	Local Session
	Remote Session

	Operator (remote site(s) that you can fully control)
	Controller (remote site(s) where you can start and stop sweeps, rescan profiles, and copy information to and from your local session)
	Observer (remote site(s) on which you can monitor scan progress)

3 Installation and Setup

This section will guide you through the process of installing and setting up PhoneSweep Gold.

3.1 System Requirements

System Requirements listed below are on a per-feature basis.

3.1.1 Distributed Requirements

You must have at least two copies of PhoneSweep Gold, each with its own Hardware License Management Device (dongle).

To set up PhoneSweep in two or more countries, please buy equipment that is geared for each country. This is especially important for modems and multi-port cards, as each country has its own electrical and communications standards.

Please see the *PhoneSweep Manual* or the Sandstorm website (http://www.sandstorm.net) for further details on modem and multi-port serial I/O card selection.

Minimum requirements (Distributed Basic - 1 Modem, Small Profiles):

- CPU: 200 MHz
- RAM: 32 MB
- Memory: 50 MB
- Network Connection: Connected to a network, either internal or external, that allows access to and/or by remote copies of PhoneSweep Gold.

Optimal requirements (Distributed Plus 4, 8, 12, 16):

- CPU: 333 MHz minimum for Plus 4 or 8;
  600-750 MHz minimum for Plus 12 or 16
- RAM: 64 – 128 MB minimum for Plus 4 or 8;
  256 MB minimum for Plus 12 or 16
- Memory: 100 MB
- Network Connection: Connected to a network, either internal or external, that allows access to and/or by remote copies of PhoneSweep Gold.

Additional Requirements: As specified in the main PhoneSweep Manual for multi-port and multi-modem connections.

3.1.2 E-mail Notification Requirements

Minimum requirements:

- Same as Distributed minimum requirements
- **Additional:** SMTP Server: You need to know the address of your outgoing e-mail server for each site that uses PhoneSweep Gold.

Optimal requirements (Distributed Plus 4, 8, 12, 16):

- Same as Distributed Optimal requirements (Distributed Plus 4, 8, 12 +16)
- **Additional:** SMTP Server: You need to know the address of your outgoing e-mail server for each site that uses PhoneSweep Gold.

3.1.3 Merged Reporting

Minimum requirements (assuming several small reports (800 unique phone numbers each)):

- CPU: 333 MHz minimum. If the total number of unique phone numbers is 10,000 or more, the CPU speed should be higher. We have noted some slowness while generating large reports with a lot of call history.
- RAM: 128 MB
- Memory: 100 MB
- Network Connection: None required

Optimal requirements (assuming large reports (10,000-20,000 unique phone numbers each)):

- CPU: 600-750 MHz, higher if you intend to use profiles containing more than 20,000 phone numbers.
- RAM: 256 MB
- Memory: 250 MB
- Network Connection: None required

3.1.4 Security

We recommend that your machine not be connected to any network, unless you are actively using the Distributed feature or the E-mail Notification feature of PhoneSweep Gold. If your machine is connected to a network, please restrict inbound access to it as much as possible. For Distributed connections, inbound and outbound access should be limited to only those machines that are part of your PhoneSweep Gold distributed network. If your local network administrators load software upgrades during the same hours as PhoneSweep is in operation, please either disconnect your machine from the network or have your machine upgraded separately. Software uploads during PhoneSweep operations have been known to cause the operating system to freeze, which could lead to profiles becoming corrupted.

3.1.5 Operating System

PhoneSweep Gold is certified to run under Microsoft Windows 95, 98, NT 4.0, XP, Windows 2000 Professional SP2 and Windows 2000 Server SP1.

We do not recommend or support using PhoneSweep Gold on Windows ME.

If you have a choice of platforms, we recommend that you install PhoneSweep on a computer using Windows 98 or Windows 2000, as these are the two most stable platforms we have found to date.

Please Note: SP2 on Windows 2000 Server has been known to cause problems. At least one customer was unable to run PhoneSweep after adding SP2. PhoneSweep only ran again when SP2 was uninstalled from Windows 2000 Server. Sandstorm is still investigating this issue.

For further information, please refer to "A cautionary note on laptop computers and Windows NT" in the *PhoneSweep Manual*.

3.2 Using PhoneSweep Gold's Distributed feature over the Internet or Corporate LAN/WAN

As long as your Internet access controls are set up properly, PhoneSweep Gold's Distributed feature can be used wherever there is Internet access. Before attempting to connect to a remote site, please find out the following:

- Are both machines on the same LAN or WAN – and if you are on a WAN, how is it set up? Does it use VPN?
- Is either machine behind a firewall?
- Is either machine behind a NAT box?

Sandstorm recommends that when you initially set up Distributed PhoneSweep, you should notify each site's network/systems administrator in case problems should arise.

3.2.1 Router (Access Lists)

Security set at the Router level is often the first line of defense for any organization. If your router has the capability (speed and memory), you can use small access lists to limit connections to your machine from only your local machine and specific remote IP addresses (with port numbers if needed) and e-mail servers you need to access.

This is not something we advise on a large network that uses a small router and large access lists. We advise that you use your firewall for this purpose instead.

3.2.2 VPN issues

Normally, VPNs should be transparent to all users. However, VPNs can be set up to allow only certain types of connections (network traffic) to occur. This can interfere with your ability to connect to a machine at a remote location on your WAN (Wide Area Network). If you find there is a problem, please contact your network/systems Administrator.

3.2.3 Firewall issues

If any copies of PhoneSweep Gold are behind a firewall, speak with your firewall administrator to create an appropriate path to the necessary machines. **Port 4322** should be open for incoming Distributed connections on all machines. The port number is configurable in the *phonesweep.ini* file, which you can find in the main PhoneSweep directory.

If you have a firewall on the same machine as PhoneSweep, you must also keep **port 4321** open for PhoneSweep to use TCP/IP for its own internal communications. This port is also configurable in the *phonesweep.ini* file. Please see the *PhoneSweep Manual*, section 3.2.2 "Firewalls and TCP/IP" for further details.

3.2.4 NAT issues

Network Address Translation (NAT) connection issues will depend on whether your local or the remote copy of PhoneSweep is behind a NAT:

- **Local copy of PhoneSweep is behind a NAT box:** You should be able to connect to any remote copy of PhoneSweep. If you are unable to make these connections, please contact your network/systems administrator.
- **Remote copy of PhoneSweep is behind a NAT box:** The type of NAT being used will determine whether or not you can resolve connection problems. Two common methods require the remote network/systems administrator to either
    - Assign you a specific port, or
    - Assign an Internet IP address to the PhoneSweep Gold machine at their remote location.
- **Multiple remote copies of PhoneSweep are behind a NAT box:** This poses some additional difficulty, as using the first solution of assigning a specific port to PhoneSweep means assigning a different port to each copy of PhoneSweep via the NAT, and making sure that the changes are noted in the *phonesweep.ini* file. If the second solution is available, you can use different IP addresses for each PhoneSweep machine, provided your remote network has spare IP addresses available. Other types of NATs may require more creative solutions in this situation.

For more in-depth information on networks, network troubleshooting and using PhoneSweep Gold's Distributed feature, please refer to Appendix A and Appendix B of this document.

3.3 Upgrading Existing PhoneSweep 4.0 Copies to PhoneSweep Gold

If you have just purchased PhoneSweep 4.0 or higher with a Gold dongle (Gold preinstalled), you can skip this section, since it is only for existing PhoneSweep installations that have upgraded to Gold.

For your convenience, the PhoneSweep Gold upgrade executable is sent to you as a .zip file, attached to an e-mail containing installation instructions. Run the unzipped executable, and then start PhoneSweep to make sure the executable was successful. You should be able to see the Distributed button ( ) along the top of the PhoneSweep user interface. The Gold manual is already on the PhoneSweep CD.

To successfully install PhoneSweep Gold via the Gold upgrade executable, you must:

- Have your dongle attached to the parallel or USB port.
- Have PhoneSweep 4.0 or higher installed on your machine, but not running.
- Have an UnZip program installed on your machine (winzip is commonly used).
- Unzip the .zip file, and run the extracted executable.

If you are running ***Windows NT or Windows 2000****, please make sure you are logged in as an Administrator*, otherwise you will be unable to upgrade to PhoneSweep Gold.

No other programs should be running, including virus checkers, as they can interfere with the Gold upgrade executable's operation. You can run a virus checker on the Gold upgrade executable before running it.

Note that *you cannot run the PhoneSweep Gold upgrade executable while PhoneSweep or any parts thereof are already running*. If an attempted installation results in an error message indicating that parts of PhoneSweep are still running, you can use the Task Manager (accessed by simultaneously pressing CTRL-ALT-DELETE) to kill the parts of PhoneSweep that are still running, including MySQLd, or you can reboot your computer.

If you have problems installing PhoneSweep Gold, please consult **Appendix B: PhoneSweep Gold Troubleshooting Guide**.

3.4 Hardware License Protection and Gold

PhoneSweep Gold adds advanced functionality to an already powerful tool via the PhoneSweep dongle. For this reason, you must have the PhoneSweep dongle (Hardware License Management Device) attached to your computer in order to access Gold features.

If you attempt to run PhoneSweep Gold without the dongle attached, it will run in **demonstration (simulation)** mode and you will not be able to see any Gold tools, nor will you be able to make any actual calls or generate merged reports. (You can still create and edit profiles, as well as generate standard and differential reports from any profiles that have already been swept).

PhoneSweep will display a warning message if it is started without the dongle in place.

3.5 Troubleshooting Gold Issues

As always, we recommend the following steps when troubleshooting any issue:

- Determine the symptoms of the problem and when they started.
- Determine how to replicate the symptoms if possible.
- Note any strange event or change in data that happened just before the problem started.

Special note on troubleshooting problems at remote PhoneSweep Gold sites:

Each remote location should have one person who can access the PhoneSweep Gold box, and can either restart the box or the PhoneSweep program if needed. Power outages, equipment failure, remote network problems and interference from other programs, such as virus checkers, all need attention on a local level.

For further information on troubleshooting PhoneSweep Gold, please see **Appendix B: PhoneSweep Gold Troubleshooting Guide**, or contact Sandstorm Enterprises technical support at *support@sandstorm.net.*

3.6 Uninstalling PhoneSweep Gold

To uninstall PhoneSweep Gold without uninstalling PhoneSweep, you need to contact Sandstorm Technical Support. Uninstalling PhoneSweep will uninstall Gold features as well, but, because we use the dongle to control Gold, you must run a special downgrade executable to remove Gold without affecting PhoneSweep. Please contact Sandstorm Technical Support for further details.

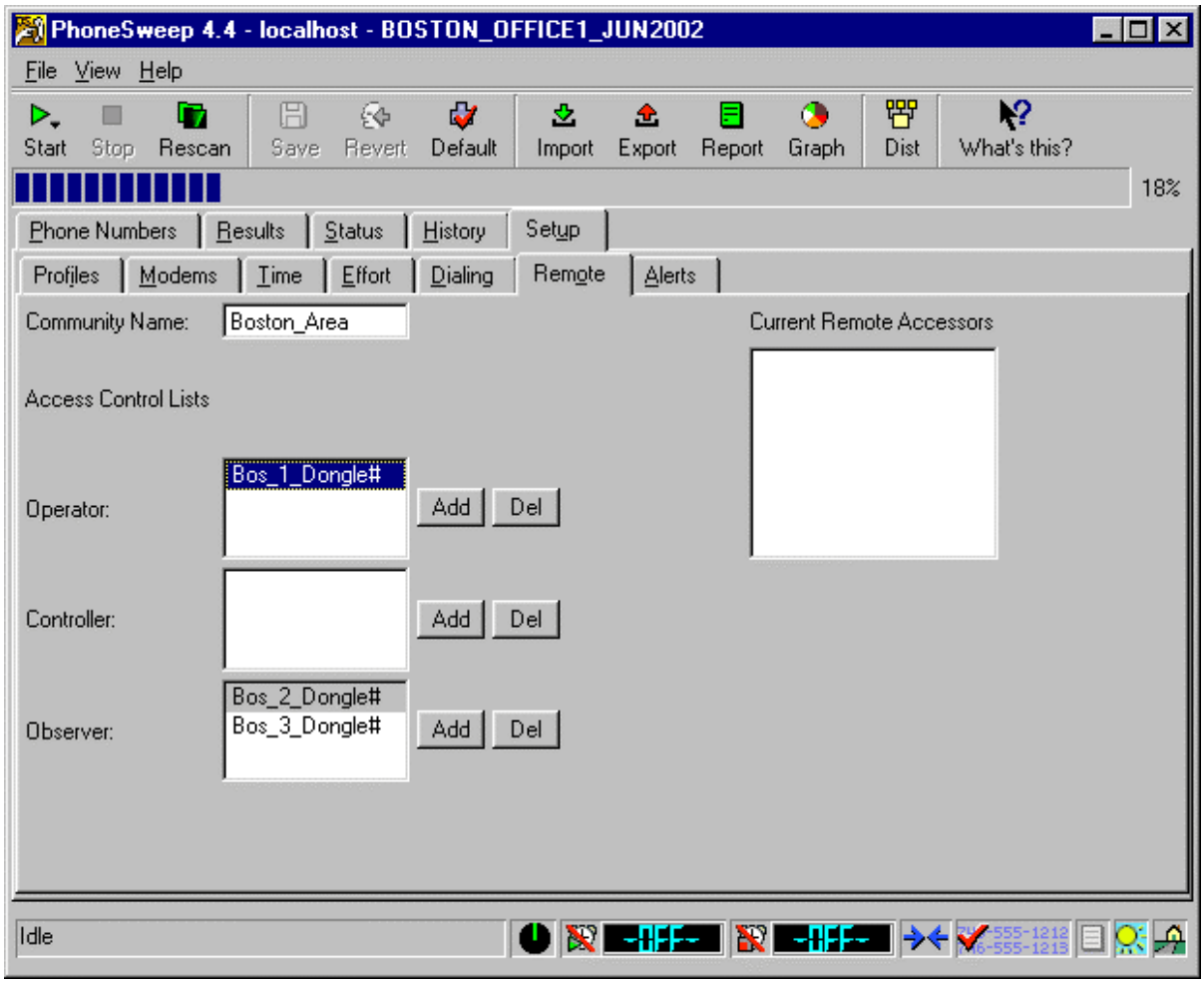
3.7 Reinstalling PhoneSweep Gold

Run the original upgrader as detailed above. If you did not save the upgrader, please contact Sandstorm Technical Support and they will send you a new one via e-mail.

If you have uninstalled PhoneSweep Gold with a downgrade executable described in the previous section, you will need an upgrade executable to reinstall Gold.

If you have uninstalled PhoneSweep Gold by removing the PhoneSweep software from your computer, simply reinstall PhoneSweep.

4 Setting Up Distributed Sweeps



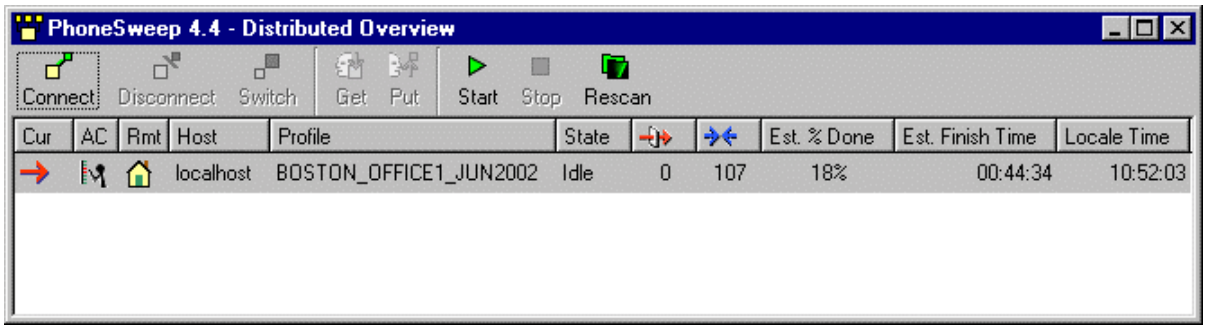
Please note the following Distributed Features:

- **Dist** (Distributed) **button,** available at top of PhoneSweep window: Displays the Distributed Overview window.

On the options **Setup->Remote** sub-tab you will see:

- **Community Name** – The community to which two or more interacting copies of PhoneSweep Gold belong. All copies of PhoneSweep Gold that need to interact with one another must be set to same community name. This community name is an encryption key, used as a security device to encrypt/decrypt the network traffic created by Gold. It should be **unique to your company.** The community name is **case-sensitive**. Sandstorm strongly recommends that you use standard secure password creation techniques (mixed case letters, numbers, and other characters) to create a unique community name for your company. Protect the identity of your company's community name as you would protect any password so that only those using PhoneSweep Gold will have knowledge of this key.
- **Access Control Lists** – The Local Manager sets which dongle IDs are allowed to remotely manage your local copy, and in what capacity.

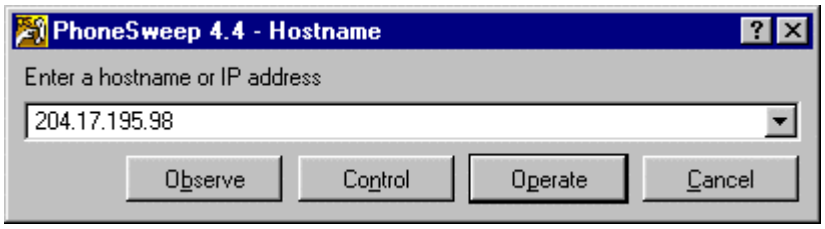
- **Current Remote Accessors** – Shows the IP address(es) of remote Gold computers currently connected to the local copy of PhoneSweep Gold.



The PhoneSweep Gold **Distributed Overview** window pops up when you select the "**Dist**" button along the top of the PhoneSweep window. This window is used to control all aspects of PhoneSweep Gold when you are acting as a Remote Manager in the capacity of Observer or Controller, according to the access granted to your dongle number by the Local Manager of each copy. The buttons at the top of the **Distributed Overview** window are as follows:

- **Connect** to a remote location.
- **Disconnect** from a currently open session.
- **Switch** between multiple operator sessions.
- **Get** a profile from a remote copy of PhoneSweep.
- **Put** a local profile to a remote copy of PhoneSweep.
- **Start** a remote sweep on the currently selected session.
- **Stop** a remote sweep on the currently selected session.
- **Rescan** to copy the current profile with current settings, to sweep the current set of phone numbers again.

Selecting the **Connect** button brings up the **Hostname** pop-up window, shown below:



To connect to a remote location:

1. Enter the **host name** or **IP address** of the remote location that you wish to connect to. Hostnames can be found by opening a computer's Control Panel and selecting *Network* or *Network and DialIn Connections*. An alternate method is to click on *Start*, select *Run*, and execute the program `winipcfg`, then select *More Info>>*. If you need more help finding host information, contact your company's internal network / PC support staff.
2. Select which level of authority you wish to connect under (Click on **Observe**, **Control**, or **Operate**). Remember that you will only be able to connect at the level of authority that the remote site's Local Manager has given your copy of PhoneSweep.

3. To view recently used hostnames and addresses click the drop-down arrow to the right of the name field, then select the recent name or address. Unsuccessful connections will not be shown on this list.

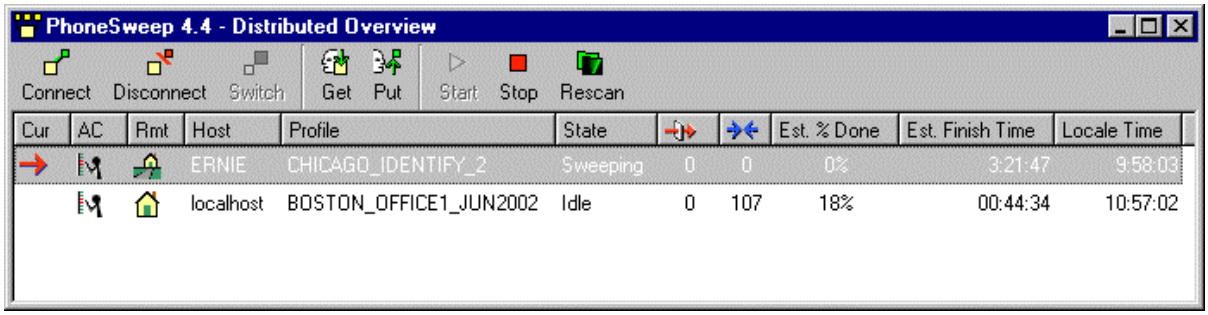
Each successful Distributed connection operates only between your local copy of PhoneSweep Gold and a given remote site. You can have an unlimited number of connections from your local copy to remote sites.

You cannot connect one remote site to another remote site using your local copy of PhoneSweep Gold.

When a new connection is successful, two things occur on your local copy of the PhoneSweep:

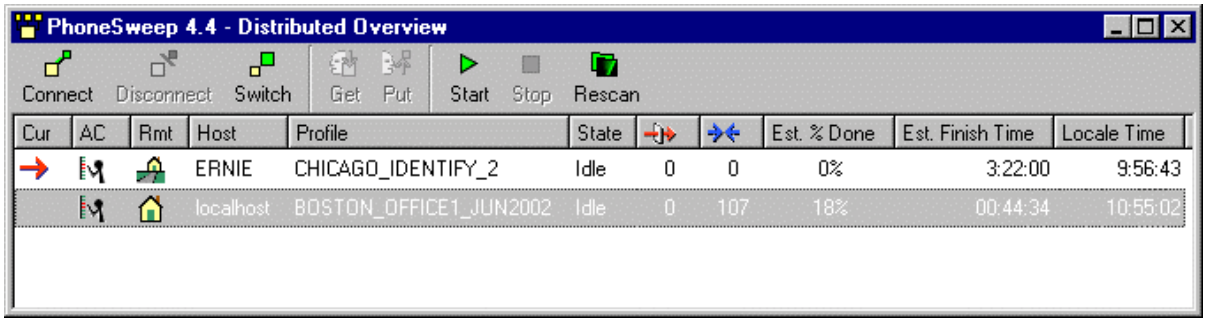
- If you have connected as an Operator, your **local user interface** will display the **remote user interface**, opening to the **Phone Numbers** tab. The top of your user interface will display the remote location's host name or IP address, and the remote location's current open profile. (See below).
- The new connection will be displayed and highlighted on the **Distributed Overview** pop-up window. (See below).

To switch between connections:



The current active connection will be highlighted in the **Distributed Overview** pop-up window.

1. Select/Highlight the connection you wish to switch to, which will un-gray the **Switch** button.



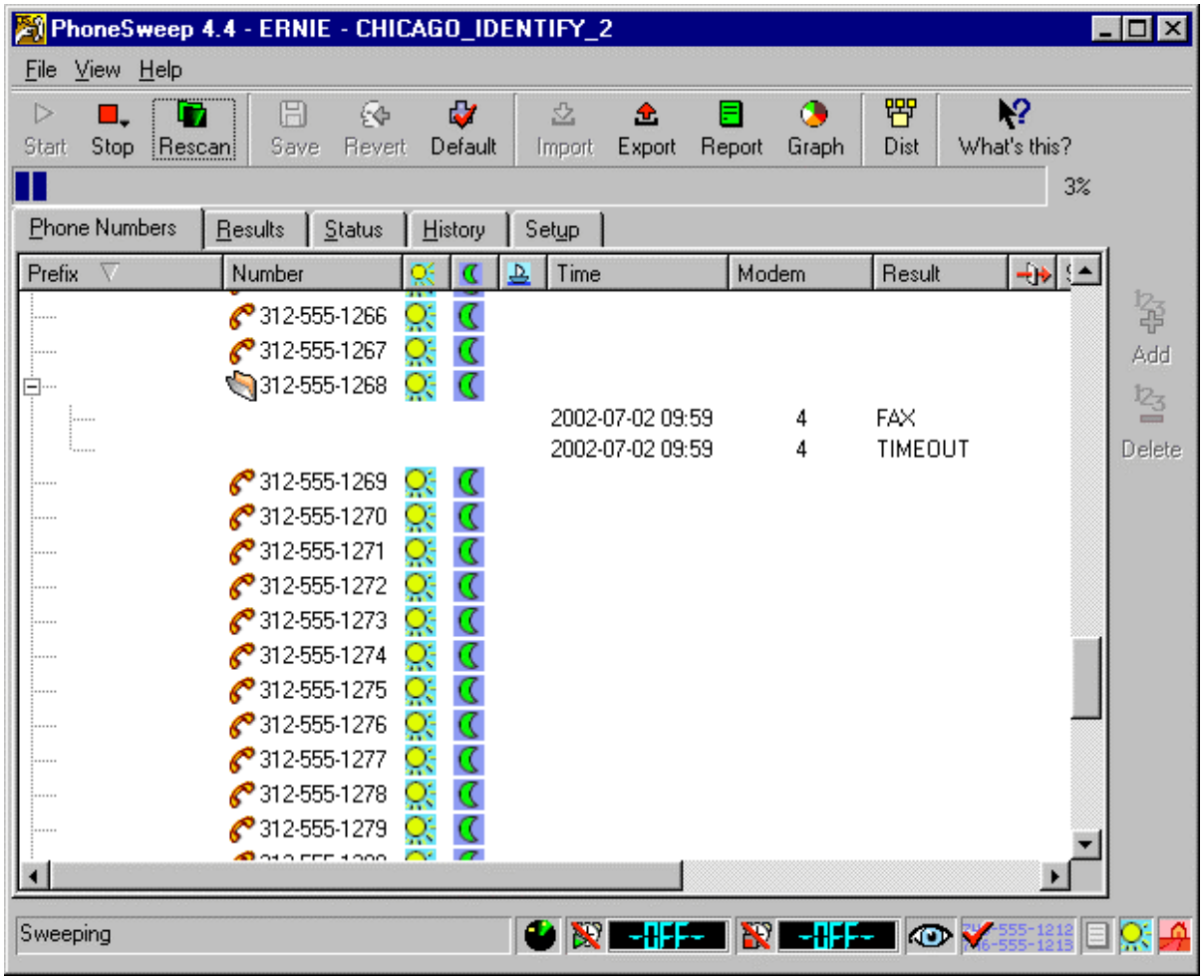
2. Click the **Switch** button to make the highlighted connection your current operational session.

Your local user interface will once again reflect the current operational session, both by displaying the new session's **host name** or **IP address** with the current open profile along

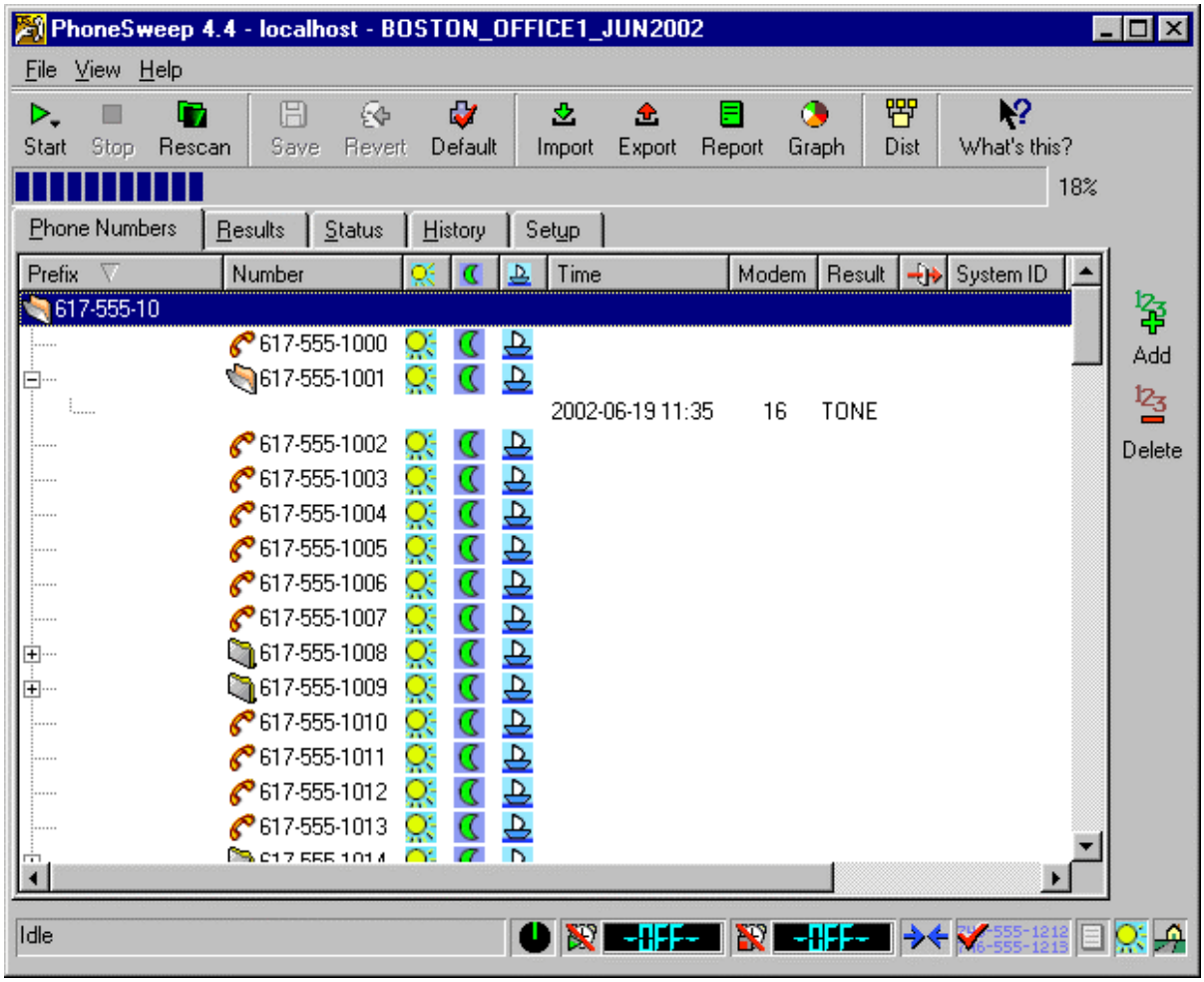
the top of the user interface; and by allowing you to Operate, Control or Observe activities at the remote copy of PhoneSweep Gold.

In the case below, we have switched between the **ernie** session in Chicago, and the **localhost** (local copy of PhoneSweep Gold) in Boston.

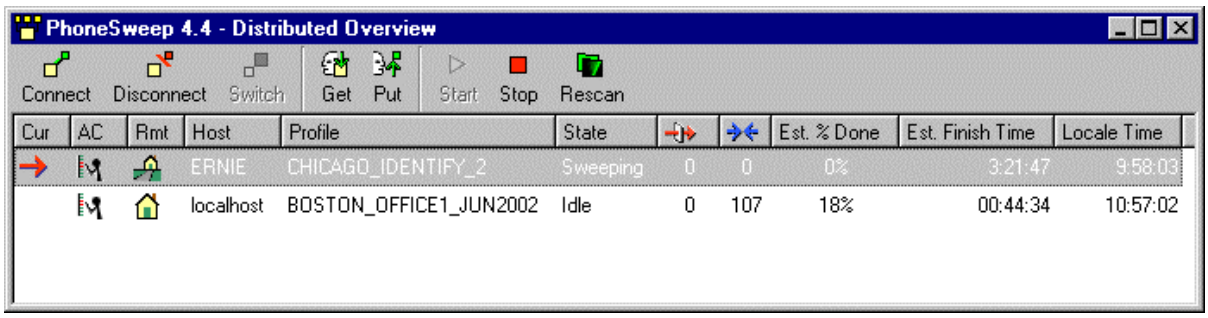
Local User Interface Before Switch:



Local User Interface After Switch:



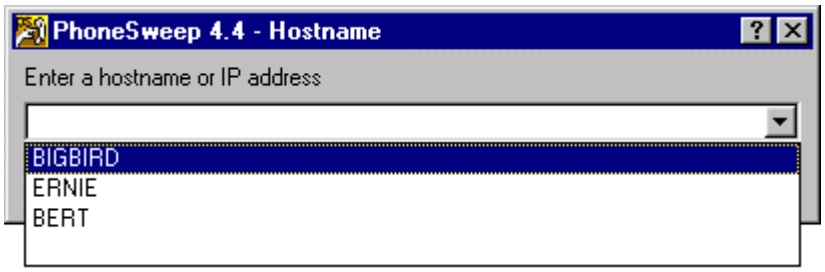
To close a connection session:


PhoneSweep 4.4 - Distributed Overview
Connect Disconnect Switch Get Put Start Stop Rescan
Cur AC Rmt Host Profile State Est. % Done Est. Finish Time Locale Time
ERNIE CHICAGO_IDENTIFY_2 Sweeping 0 0 0% 3:21:47 9:58:03
localhost BOSTON_OFFICE1_JUN2002 Idle 0 107 18% 00:44:34 10:57:02

1. Select the **Dist** button from the main PhoneSweep screen to view the Distributed Overview window.
2. **Disconnect** will only work on the currently selected session connection.
3. Make sure that the session you want to terminate is selected.
4. Click on the **Disconnect** button. You cannot disconnect from your local (localhost) connection, as that is your machine.

To re-connect to a closed session: PhoneSweep retains a list of the four most recently opened connections. Unsuccessful connections are not stored on this list.

You can re-open these connections by selecting the **Connect** button on the **Distributed Overview** pop-up window, in order to bring up the **Hostname** pop-up window below:



1. Click on the down arrow to the right of the Entry field to bring up the list of previous successful connections.
2. Select the connection you wish to re-connect to.
3. Click on the level of access you wish to have for that connection (provided you select an allowed level of access).

To Transfer information between your Local copy of PhoneSweep and the Remote copy of PhoneSweep Gold:

Select the **Dist** button from the main PhoneSweep screen to view the Distributed Overview window.

- Click the **Get** button: to transfer a profile from the remote copy of PhoneSweep Gold to your local copy of PhoneSweep Gold.
- Click the **Put** button to transfer a profile from your local copy of PhoneSweep Gold to the remote copy of PhoneSweep Gold.

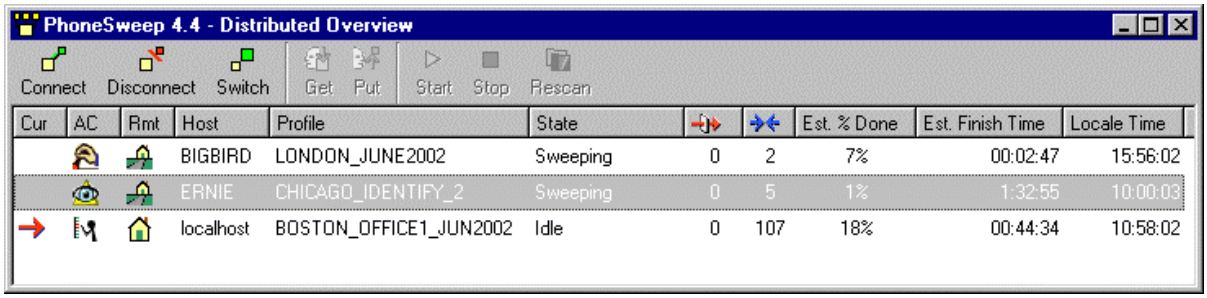
To Stop, Start and Rescan Sweeps via the Distributed Overview window:

Select the **Dist** button from the main PhoneSweep screen to view the Distributed Overview window.

- Click the **Start** button: To start a sweep on the current active connection session.
- Click the **Stop** button: To stop a running sweep on the current active connection session.
- Click the **Rescan** button: To copy and open to the current open profile on the current active connection session.

For more in-depth information on setting up and managing Distributed PhoneSweep, please see Section 4.1 “Setting Up And Managing Distributed PhoneSweep” below.

4.1 Setting Up And Managing Distributed PhoneSweep



4.1.1 What does Distributed allow me to do?

Distributed allows you to operate (via PhoneSweep Gold itself) remote copies of PhoneSweep Gold at one of 3 levels of interaction.

- Observer: ()
  - Can observe scan progress at remote locations via the Distributed Overview.
  - Cannot view any other activities.
- Controller: ()
  - Can start and stop sweeps.
  - Can rescan profiles.
  - Can transfer profiles between local and remote copies of PhoneSweep Gold.
  - All Observer functionality.
- Operator: ()
  - Has total remote control over this copy of PhoneSweep Gold.
  - Can edit remote access lists.
  - All Controller functionality.

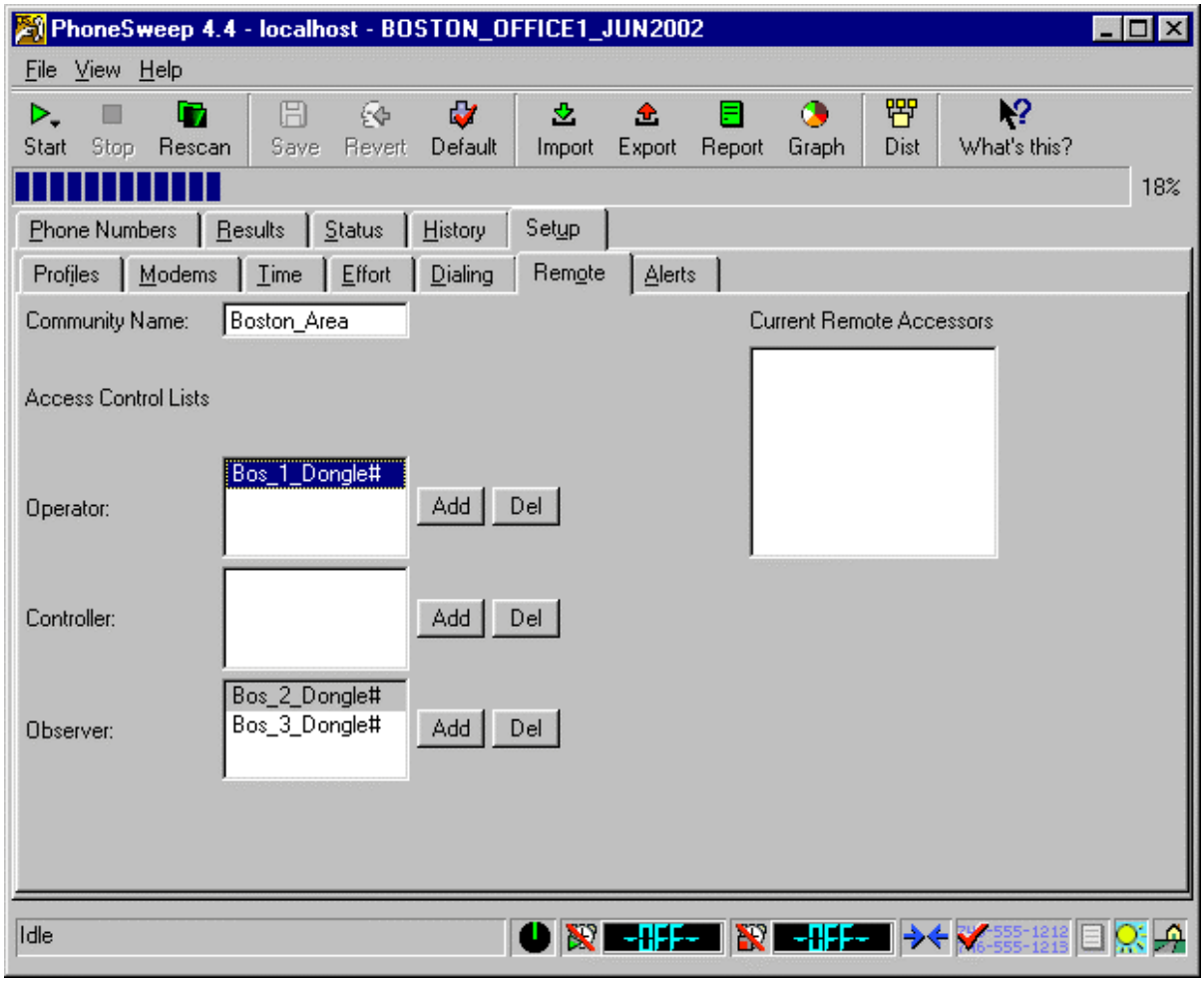
PhoneSweep Gold does this through the use of Access Lists, which are applied locally to each copy of Gold (see next section). Whenever you make a new connection session from your local copy of Gold, the remote copy of PhoneSweep Gold compares both your dongle number and Community Name to those listed in its **Setup->Remote** sub-tab.

You can make as many connections from your local copy of PhoneSweep Gold as you have computing power to handle.

You cannot create a remote session between two remote copies, even if you have Operator access to both remote copies.

With Operator control, you can change the access list on a remote copy of PhoneSweep Gold.

4.1.2 PhoneSweep Distributed Access Control



Access Control Lists let you set which and how much control remote copies of PhoneSweep Gold have over your local copy. This is found on the **Setup->Remote** sub-tab.

Gold access control lists are based upon both the Remote Manager's dongle number and the community to which each dongle belongs. Both local and remote dongles must belong to the same community.

Setting access control on a local level:

- Ensures that only Gold dongles with defined access levels can connect to a given copy of Gold to perform specific functions.
- Allows the Local Manager to edit or revoke any access, should the need arise. If you are connected to a remote copy as an Operator, you can also change the access control lists for that copy.
- **Initial setup requires that Access Control Lists at each remote site must be set up at that site,** in order for you to connect from your local copy of PhoneSweep.
- **Subsequent to initial setup, anyone who has Operator access to a remote copy of PhoneSweep Gold can change the access list on a remote copy of Gold.**

Using both the dongle number in conjunction with a Community Name for authentication adds a second level of security in ensuring who can access a given copy of Gold.

This also allows you to also break up a larger number of dongles within your organization to finite communities.

Each copy of Gold has two modes of interaction with other copies of Gold.

- **Local Manager:** You control the copy of PhoneSweep Gold on your site, which includes initially setting access levels for other copies of Gold to remotely manage/access your local copy.
- **Remote Manager:** You remotely manage/access other copies of PhoneSweep Gold at any level of access.

You cannot access or manage any remote copy of PhoneSweep Gold unless you have been granted permission by the Local Manager for that copy. The Local Manager can grant one of three remote access levels to Remote Managers: Observer, Controller, or Operator (see previous page for definitions).

4.1.3 Before Setting Up

Access control lists for each copy of PhoneSweep Gold must be set up locally. Once you have set up access control lists at each location, an identified Remote Manager/Operator can change access settings remotely.

For both physical security and troubleshooting, Sandstorm recommends the following when setting PhoneSweep Gold up at a remote location:

- Place PhoneSweep Gold on a dedicated machine in a secure location, ensuring that no other software, including virus checkers, is running on that machine.
- If you do not have a secure location, Sandstorm recommends that you determine whether PhoneSweep Gold will operate properly with a native screensaver, or that you use ScreenLock (http://www.screenlock.com).
- Designate at least one ***trusted*** person who can reach the remote site easily. This person will be needed to check on PhoneSweep Gold's functioning and to troubleshoot physical issues (e.g. to turn the machine on after a power outage). This should be the same person who helps you set up initial access via PhoneSweep.
- Network access to this machine must be limited so that only permitted IP addresses and ports can communicate with the local machine. This can include using a Firewall on the PhoneSweep Gold machine. Port 4321 needs to be open for internal PhoneSweep operation, while port 4322 needs to be open for remote Gold communication. You can reset both ports through the *phonesweep.ini* file.
- Local Managers at each remote site should perform an initial test sweep of their site so they can adjust PhoneSweep settings as needed. You should record any unique settings specific to each site.

For your convenience, **please note** that you do not need to have the user interface running on the remote location when you are connected to that location. You can start the PhoneSweep Gold engine without the user interface from an MSDOS window with the command: `phonesweep.exe -nogui`.

4.1.4 Setting up

When planning your PhoneSweep Gold distributed network:

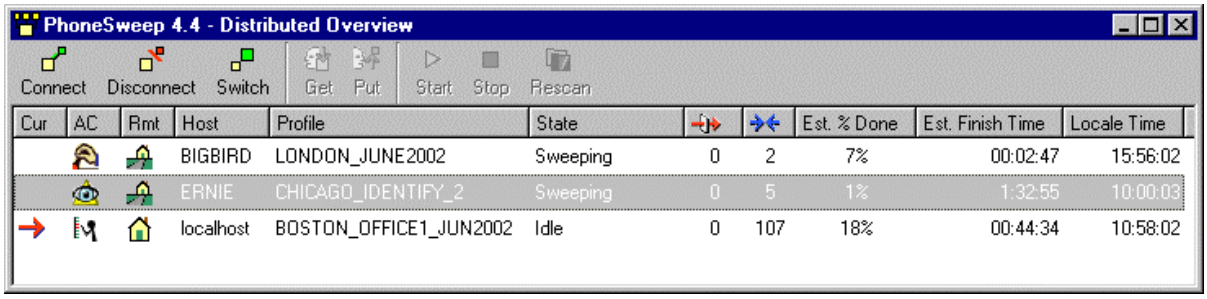
1. Determine which remote copies of PhoneSweep Gold will have access to other copies of PhoneSweep Gold, and what level of access each shall have.
2. Determine whether all dongles in your organization will belong to the same community, or if you plan to group certain dongles into individual communities.
3. Make a list of host names, IP addresses, dongle numbers and what group or set each belong to.
4. Assign a unique Community Name to each group or set of PhoneSweep Gold copies that will be communicating with one another using the Distributed feature.

If you need to control two or more different communities from your machine, you can change your community name on your copy of PhoneSweep Gold as needed, and select the **Save** button at the top of your copy of PhoneSweep. **Note:** Your dongle number must be listed on the remote copies of PhoneSweep Gold for all communities that you will be controlling.

The Local Manager for each copy must start up PhoneSweep Gold, and on the **Setup->Remote** sub-tab, enter the agreed-upon Community Name for that copy of PhoneSweep, and the dongle numbers permitted access to the local copy at the appropriate level(s) of access.

While the Local Manager(s) are setting up access at their remote site(s), you may want to use your copy of PhoneSweep Gold to test remote access to those sites.

4.1.5 Managing Distributed Session Connections



All sessions (connections) opened via the **Hostname** pop-up window will appear listed in the **Distributed Overview** window. When a session is terminated (disconnected) it will be removed from this list; however, the remote copy of PhoneSweep will continue to operate.

The highlighted session above (Hostname: Ernie) has been selected for further management via the Distributed Overview window. Any actions performed in the **Distributed Overview** window will be made against that session.

The session with an arrow to the left (Hostname: localhost) is the current active session in the main PhoneSweep window. You will see the host name and the current open profile for that remote copy of PhoneSweep along the top of the main PhoneSweep window. Any actions performed in the main PhoneSweep window will be for that copy of PhoneSweep.

You can highlight any session in the Distributed Overview by clicking on it.

To perform any action on a remote session, select the session from the list before performing one of the following operations:

- **To start or stop a sweep on a remote or local session:** Click **Start** to begin a sweep, or **Stop** if already sweeping. Only Operators and Controllers can start and stop sweeps.
- **To switch to another remote session as Operator:** Click **Switch**. If you are not currently an Operator on that session, you will be notified that you are switched to an Operator. If you don't have Operator privileges on that remote site, you cannot switch to it as an Operator.
- **To create a profile containing the phone number list in a remote or local session's current profile, with the current scanning preferences:** Click **Rescan**. This works just like **Rescan** on a local copy of PhoneSweep. Only Operators and Controllers can rescan profiles on remote sessions.
- **To copy a profile from the local PhoneSweep Gold to a remote PhoneSweep Gold:** Click **Put**. PhoneSweep Gold will prompt you to select the profile to copy, and then to type a name for the new profile. Only Operators and Controllers can use the Put action on remote sessions.
- **To copy a profile from a remote PhoneSweep Gold to your local PhoneSweep Gold:** Click **Get**. PhoneSweep will prompt you to select the profile to copy, and then to type a name for the new profile. Only Operators and Controllers can use the Get action on remote sessions.
- **To disconnect from a remote session:** Click **Disconnect**. PhoneSweep Gold will prompt you to confirm the disconnection. After disconnecting from a remote session, the remote PhoneSweep Gold will continue to operate even though you are no longer connected to it.

4.1.6 Importing and Exporting with Remote Sessions

You can import phone numbers and username/password files, and export phone numbers and call history, to and from remote sessions using PhoneSweep Gold. You must be connected as an Operator to the remote session. If the remote session is not already the current session, switch to it using the **Switch** button on the Distributed Overview. You can then click on the **Import** or **Export** buttons on the main PhoneSweep window. Importing and exporting both work a little differently over remote connections, than just importing and exporting files to and from the local session:

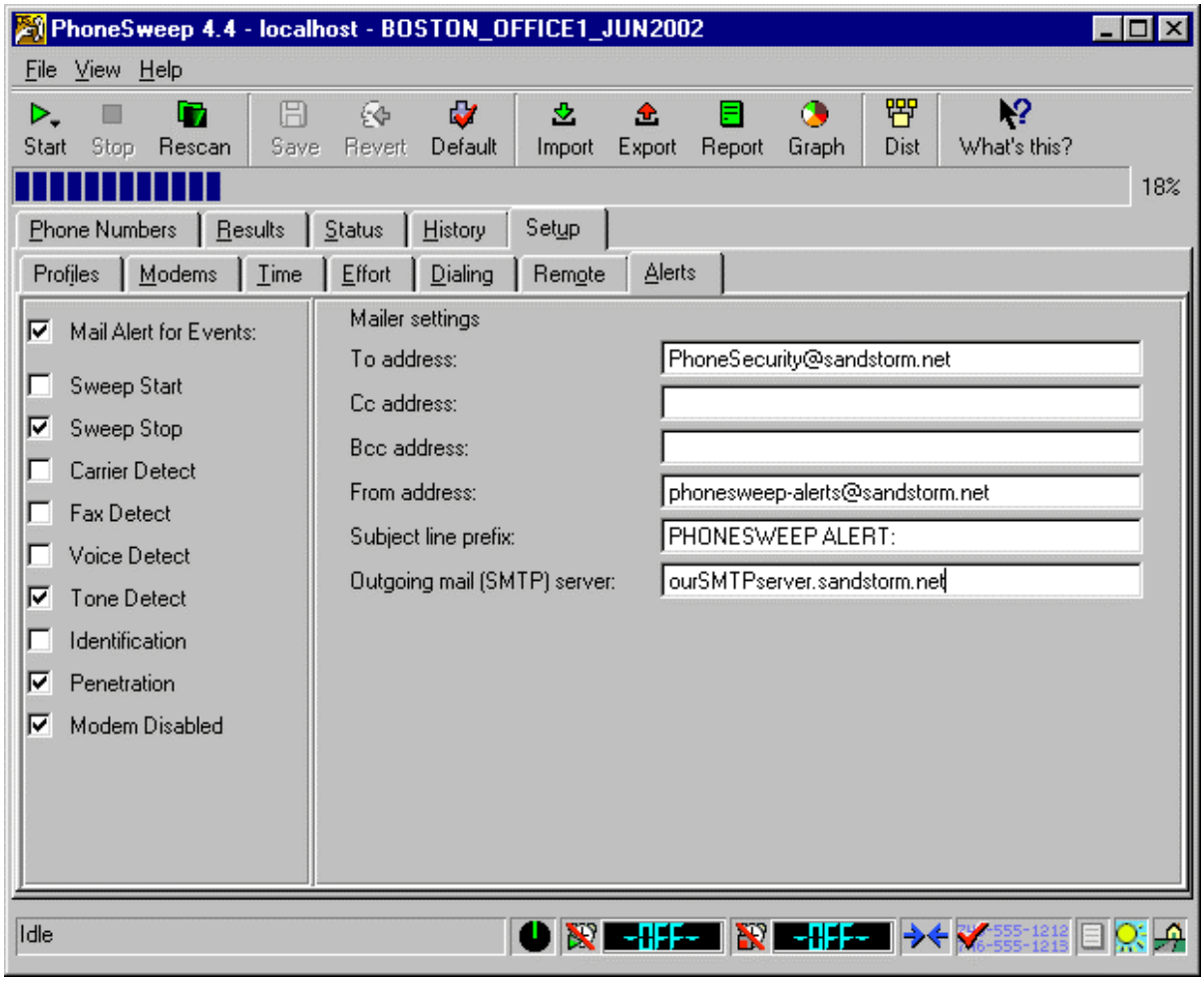
- **Import** sends data from a file on the local session's machine to the remote session.
- **Export** saves data from the remote session to a file on the local machine.

4.2 Possible Distributed PhoneSweep Injuries

- **Mistyped Dongle Numbers.** Dongle numbers for Remote Managers/Accessors must be allowed access on the copies you want to remotely control. See **Section 4.1, "Setting Up And Managing Distributed PhoneSweep"**, for setting this up properly.
- **Mistyped Community Names.** All copies of PhoneSweep Gold that need to communicate must be part of the same Community Name. See **Section 4.1, "Setting Up And Managing Distributed PhoneSweep"**, for setting this up properly.

- **Mistyped IP address or host name.** Check with your system administrator for the proper IP address or host name of the recipient PhoneSweep Gold machine. See **Section 4.1, "Setting Up And Managing Distributed PhoneSweep"** for setting this up properly.
- **Firewall not configured properly.** Ensure that all firewall administrators at all distributed sites have the proper port setup for Gold to operate. See **Section 3.2.3, "Firewall Issues"** for details on the proper firewall configuration.
- **Proper access type not set up prior to connection.** Proper access must be defined on the recipient copy of PhoneSweep Gold (Operator, Controller or Observer) prior to remote access taking place. See **Section 4.1, "Setting Up And Managing Distributed PhoneSweep"** for setting this up properly.

5 Setting Up And Managing Automatic E-mail Notifications



PhoneSweep Gold's E-mail Notification feature will send e-mail based on various criteria, defined in this section.

- **Mail Alert for Events:** Checking the *Mail Alert for Events:* box enables the Gold E-mail Notification option to send out notifications when PhoneSweep encounters any of the checked alerts listed below. If this box is not checked, no e-mail alerts will be sent, even if the separate alerts are checked. Alert settings are unique to each profile. Default alert settings are defined in the *phonesweep.ini* file.
    - **Sweep Start**: E-mail will be sent when a sweep starts, whether it is started manually or due to a scheduled start.
    - **Sweep Stop**: E-mail will be sent when a sweep stops, whether it is stopped manually, ended normally because there are no more numbers to dial, or due to a scheduled stop.

- **Carrier Detect**: E-mail will be sent when a CARRIER call result is returned during a sweep.
- **Fax Detect**: E-mail will be sent when a FAX call result is returned during a sweep.
- **Voice Detect**: E-mail will be sent when a VOICE call result is returned during a sweep. **USE CAUTION when selecting VOICE for E-mail notifications** – Make sure it is not a common event of the phone system you are sweeping.
- **Tone Detect:** E-mail will be sent when a TONE call result is returned during a sweep.
- **Identification:** E-mail will be sent when a system is successfully identified during a sweep.
- **Penetration:** E-mail will be sent when a system is successfully penetrated during a sweep.
- **Modem Disabled:** E-mail will be sent when a modem is disabled during a sweep. This can happen after repeated NO DIALTONE results or if the modem stops responding.

- **Mailer Settings:**
  - **To address:** E-mail address for primary e-mail notification recipient(s).
  - **CC address:** E-mail address for secondary e-mail notification recipient(s).
  - **BCC address:** E-mail address for Blind Carbon Copy e-mail notification recipient(s).
  - **From address:** This is the e-mail address that will appear in the From: header of the e-mail notifications. You may use the default, or customize it to your requirements.
  - **Subject line prefix:** Beginning text of the Subject: header for all PhoneSweep e-mail notifications. The type of notification will follow the prefix in the Subject header.
  - **SMTP Server:** This is your outgoing e-mail server. You can discover this by looking through the setting of your regularly used e-mail program (Outlook Express, Netscape Mail, Eudora, or other e-mail program) or by asking your e-mail support staff.

The body of the e-mail message sent will contain details about the event. At this time, the body is not configurable by the user.

5.1 Setting Up A Test E-mail Notification

We recommend that before you set up Gold E-mail Notification, you perform an initial survey of each phone network to avoid setting e-mail notification for common events. Selecting e-mail notification for common events can unintentionally generate hundreds or thousands of e-mail messages to yourself and other designated recipients. This could place a strain on your e-mail server and fill your mailbox during an overnight scan.

For example, if you have 10,000 phone numbers, and 9,000 of them are voice lines, if you set e-mail notification for voice lines, you will receive 9,000 e-mail messages at the rate of approximately 1 per minute per modem.

To assure yourself of the accuracy and reliability of your phone system survey, please speak with your telecom manager or other authority on your phone system. Having a general overview of your system beforehand also helps you to better interpret sweep results.

5.1.1 Verify e-mail addresses and notify recipients prior to scanning.

We recommend that you **verify all e-mail addresses prior to use with Gold's e-mail notification** feature. One way of performing this verification is to send e-mail from your account to other message recipients and make sure that the owner of each address understands what they are about to receive.

5.1.2 Test sweep to verify e-mail notification addresses

Once you have completed your phone system survey, we advise you to set up a small profile to sweep about 10 numbers, which should include the following types of lines:

- A number known to reach voice-mail
- A known disconnected or unassigned phone number
- A data-only modem
- A fax/modem
- A fax machine

Understanding how your organization's PBX and phone system operate will assist you in interpreting and evaluating the information collected in a PhoneSweep scan and aids you in making decisions based on the data collected. For instance, it lets you estimate how many e-mail notification messages you will receive for this scan. See Section 10: "Evaluating the Results of Your Scan" in the *PhoneSweep manual*.

5.2 Sample Gold E-mail Notification Message

This is a sample message automatically generated by PhoneSweep Gold's e-mail notification feature.

```
From: phonesweep-alerts@sandstorm.net
Sent: Monday, June 17, 2002 10:29 AM
To: security-monitor@bogus.netaddress
Subject: PHONESWEEP ALERT:Carrier detected!

Mon Jun 17 10:29:41 2002

Carrier detected!
555-1234
```

5.3 Possible E-mail Notification Injuries

By setting up automatic e-mail notification, you accept responsibility for all possible e-mail injuries that may result. To prevent these injuries, you must always ensure that you only send out e-mail notifications on rare events, that your list of e-mail notification recipients is always current, and addresses are spelled correctly.

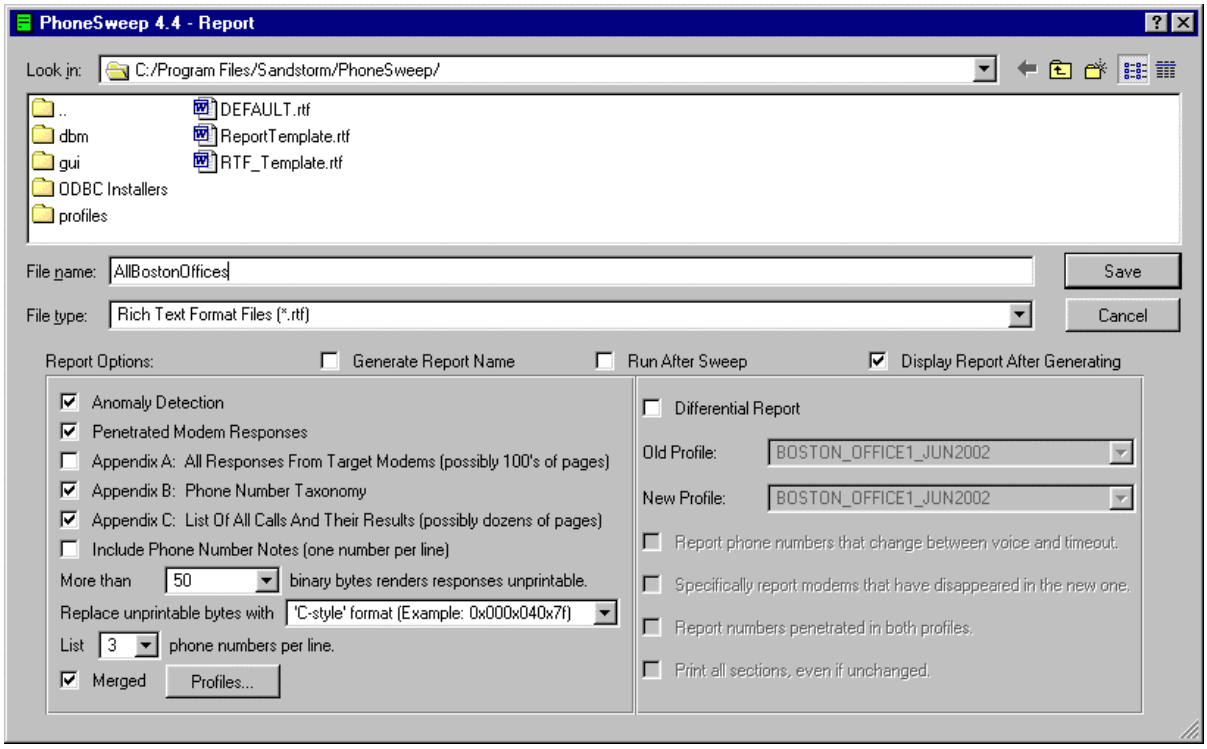
Possible testing injuries include, but are not limited to:

- **Overtaxing your mail server** if you have E-mail Notification set to notify on common events. (If 20,000 of 25,000 numbers are voice and your copy of PhoneSweep is set notify on voice, you could quickly fill up your mail box with 20,000 messages in the course of the scan.)
- **Bounced e-mail messages** from e-mail addresses that are no longer active or where there is a typo in the e-mail address.
- **Notifying the wrong persons** of problems (incorrect address entry or being given the wrong contact person to notify, or you are not notified of changes in personnel or position duties.).
- **Incorrect outgoing mail (SMTP) server** defined. Verify that you have the proper SMTP server defined, or no mail will be sent from PhoneSweep Gold.

Issues which should be considered beyond your control are:

- Not receiving e-mail notifications if a local area network, e-mail or paging server should go down.
- Other equipment, network, power or software failure.
- Domain Registration and/or Domain Name Server (DNS) issues.

6 Generating Merged Reports

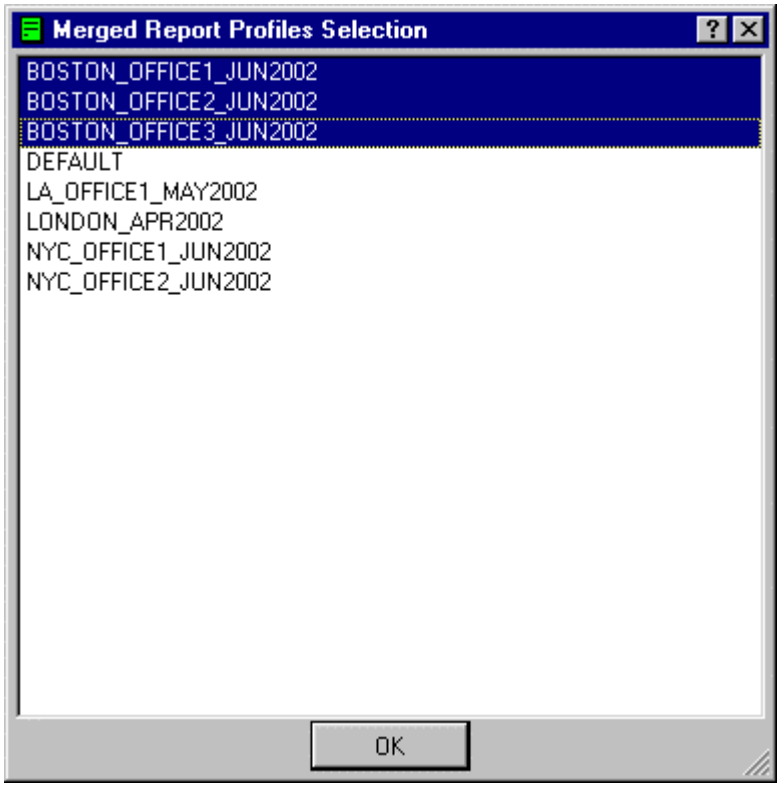

PhoneSweep 4.4 - Report
Look in: C:/Program Files/Sandstorm/PhoneSweep/
..
dbm
gui
ODBC Installers
profiles
DEFAULT.rtf
ReportTemplate.rtf
RTF_Template.rtf
File name: AllBostonOffices
Save
File type: Rich Text Format Files (*.rtf)
Cancel
Report Options:
Generate Report Name
Run After Sweep
Display Report After Generating
Anomaly Detection
Penetrated Modem Responses
Appendix A: All Responses From Target Modems (possibly 100's of pages)
Appendix B: Phone Number Taxonomy
Appendix C: List Of All Calls And Their Results (possibly dozens of pages)
Include Phone Number Notes (one number per line)
More than 50 binary bytes renders responses unprintable.
Replace unprintable bytes with 'C-style' format (Example: 0x000x040x7f)
List 3 phone numbers per line.
Merged
Profiles...
Differential Report
Old Profile: BOSTON_OFFICE1_JUN2002
New Profile: BOSTON_OFFICE1_JUN2002
Report phone numbers that change between voice and timeout.
Specifically report modems that have disappeared in the new one.
Report numbers penetrated in both profiles.
Print all sections, even if unchanged.

Merged Reporting allows you to merge sweep results from multiple profiles into a single comprehensive report. The format of a merged report is similar to a regular PhoneSweep report, with the following content differences:

- All of the merged profiles' names and notes are listed in the Executive and Engineering Summary sections of the report.
- Elapsed time and percentage data is combined for all profiles.
- Phone number lists and call results tables and sections are presented as if all numbers and results were contained in one large profile.

The **Merged Profiles** settings are on the lower left hand of the **Report** pop-up window. Clicking the **Merged** box to check it un-grays the **Profiles** button.

Clicking the **Profiles** button brings up the **Merged Report Profiles Selection** pop-up window (see next figure), which displays a list of all profiles as seen on the **Setup->Profiles** sub-tab.



The **Merged Report Profiles Selection** pop-up window allows you to select the profiles you want to merge. We recommend that you choose profiles that do not contain the same phone numbers. The percentages calculated in the report apply to unique phone numbers, and duplicate phone numbers may affect the accuracy of these percentages. If you wish to compare profiles containing the same phone numbers, a Differential report will provide more meaningful results. See the *PhoneSweep manual* for more information about running Differential reports.

The final merged report will contain both the names and associated comments from each of the profiles you select. Phone number lists, call result lists and sweep elapsed times from the individual profiles will be combined into single groupings, as though the sweeps all occurred under the same profile.

To generate a merged report:

1. Select the **Merged** check box.
2. Select the **Profiles** button to bring up the **Merged Report Profiles Selection** pop-up window, which displays a complete list of profiles.
3. Highlight the profiles you want to merge together, then select the **OK** button. This returns you to the Report window.
4. PhoneSweep will automatically generate a file name for the **Merged** report using the full or partial names of the selected profiles. If you wish to supply your own name, uncheck the **Generate Report Name** checkbox, and type in the filename of your choice.
5. Select the report options you want displayed on your merged report, then click the **Save** button.

If you want to merge profiles created on remote copies of PhoneSweep Gold, you can use the **Get Profile** feature to transfer the profile to your local machine first. See **Section 4.1.5, Managing Distributed Session Connections**, for instructions on how to do this.

6.1 Possible Merged Report Injuries

Merged Reports can become quite large as multiple reports are merged into one. In the case of merging reports containing 20,000 numbers apiece, you will notice some slowness. Some machines may not have enough CPU and RAM to handle such a large operation.

Before printing, be sure to check the size of the report to be prepared, to refill any paper, and to let other users of the printer know that it may be in use for a while.

Appendix A: PhoneSweep Gold FAQ

The PhoneSweep Gold FAQ is a collection of Frequently Asked Questions and answers about normal PhoneSweep Gold operations. For information on diagnosing problems and troubleshooting, please see **Appendix B: PhoneSweep Gold Troubleshooting Guide**.

This FAQ is arranged by topic. If a specific question and answer belongs in more than one category, it will appear in each.

Distributed PhoneSweep

How is Distributed beneficial to me?

PhoneSweep Gold's Distributed feature allows the freedom to:

- Directly operate most or all PhoneSweep functions at multiple remote locations.
- Transfer information about sweeps at remote locations to one central location for further processing or forwarding to a new location.

This frees up the need for other personnel in all but the most critical situations where hands-on troubleshooting is required.

What are the advantages and disadvantages of choosing one access control level over another?

- The main advantage of **Observer** mode is that it loads very quickly, since all of the data appearing on the PhoneSweep user interface does not have to be sent over the network. This allows you to use Observer mode to quickly check an ongoing scan's progress. The disadvantage of Observer mode is that you have no control over the remote session. However, this may be considered an advantage for security reasons, depending on your organizational structure.
- Advantages of **Controller** mode are similar to Observer mode, in that you can quickly load a remote session for monitoring purposes. You also have more control over the remote session, in that you can start and stop sweeps, rescan profiles, and transfer profiles between the local and remote sessions. The disadvantage of Controller mode is that you do not have total control over the remote session. However, this may be considered an advantage for security reasons, depending on your organizational structure.
- The main advantage of **Operator** mode is that you have full control over the remote copy of PhoneSweep Gold. The disadvantage of Operator mode is that it can be slower to load remote sessions, due to more data sent over the network for display on the main user interface. Also, it may be more of a security risk.

Why do I need someone local to perform a sweep at remote sites?

Sandstorm highly recommends that customers perform an initial sweep of 10 known numbers (voice, fax, carrier and one unassigned number) at every new site to be swept. Every phone

system is set up differently and testing helps you to adjust PhoneSweep Gold's settings before finding out you need to adjust them during a live sweep.

Performing a test sweep can also reveal phone line configuration and line noise issues.

Please refer to the main *PhoneSweep manual* for further testing information.

Why do I still need a Local Manager or someone with access to the PhoneSweep Gold Machine and PhoneSweep at each remote site?

Depending on your organization's configuration and needs, either you (by going to the remote site) or a Local Manager can initially set up and test the PhoneSweep Gold machine and lines.

However, in the case of emergency situations (such as a power outage shutting down the machine running PhoneSweep Gold), someone needs to be on-site to monitor and respond.

The need for on-site personnel in case of emergencies or troubleshooting needs is a situation faced by all remote-style technologies. After the initial setup, having someone locally available who can access the technology in emergencies is invaluable. Even if someone is not available at the remote site, some situations may require that personnel travel there.

Some of this need can be alleviated if you have an alternative way to remotely check the box PhoneSweep is running on (such as remotely rebooting the machine or auto-reboot), and possibly an alternative way of accessing the machine and PhoneSweep (such as a backup internet circuit or dial-up).

Why does operation on my remote copy of PhoneSweep Gold seem so slow?

Several factors can determine the speed of a distributed connection:

- Machine configuration. Do both PhoneSweep Gold machines have enough CPU and memory for what you are doing?
- Size of connections (either local or remote site), how many users are using the same Internet connection, and the type of information being passed.
- Time of day. Most Internet traffic tends to rise beginning late afternoon and continuing into the evening.
- Problems on your LAN, WAN or the Internet at large.

Once you have ruled out issues pertaining to the PhoneSweep Gold machines, take what information you can to your network/system administrator for further troubleshooting. See also **Distributed Troubleshooting**.

E-mail Notification

How is E-Mail Notification beneficial for my organization?

Real time e-mail notification allows you to catch events as they occur, depending on your use of PhoneSweep Gold.

- Catch unauthorized modems in the act, so you can obtain evidence and authorization for further investigation and processing.

- Determine when a critical service is not responding or has not responded for a period of time.

I am getting thousands of e-mail messages! How do I stop this from happening?

First, stop the current sweep immediately. The primary cause could be that you set PhoneSweep Gold e-mail notification to notify you of common events found on the phone system you are sweeping, (such as notifying when finding carrier when you are sweeping a system that has a high number of dial-up systems).

If the e-mails continue after you both stop the sweep and shut down PhoneSweep, then your e-mail server may be broken, or there are still pending e-mails in the mail server queue. You should contact your network/systems/mail server support staff immediately. You may also wish to verify the headers on the e-mails to ensure they are PhoneSweep Gold e-mail notifications. There is always the possibility that someone else's e-mail server is broken.

What is SMTP and how do I get the address for my SMTP server?

SMTP stands for Simple Mail Transfer Protocol. It is the protocol used by most mail applications to transfer mail between mail hosts or servers. You can discover this by looking through the setting of your regularly used e-mail program (Outlook Express, Netscape Mail, Eudora, or other e-mail program) or by asking your e-mail support staff.

Merged Reports

What can Merged Reporting do for me?

The capability to merge information from multiple sweeps streamlines the reporting process for large organizations. Comprehensive reports provide a single point of reference when reviewing phone line security on the enterprise level.

Why is Merged Report Generation so slow?

If you are pooling together information from several profiles with over 10,000 phone numbers each, you may notice some slowness even with the optimal recommended CPU and RAM. PhoneSweep must pull together, then process the information from all selected profiles before it can generate the final Merged Report.

Why are the percentages not what I expected in my Merged Report?

Check to see whether you have many phone numbers in common between the profiles you have selected for the Merged Report. We recommend that you choose profiles for Merged Reports that do not contain the same phone numbers. The percentages calculated in the report apply to unique phone numbers, and duplicate phone numbers may affect the accuracy of these percentages. If you wish to compare profiles containing the same phone numbers, a differential report may provide more meaningful results. See the main PhoneSweep manual for more information about running differential reports.

Is there Merged Charting?

Often merged reports produce results that are too large for Microsoft Excel 2000 to handle. Therefore, at this time, automatic charting of merged reports is not available.

Improving Distributed PhoneSweep's Performance

To improve PhoneSweep Gold's distributed performance, please keep the following in mind:

- ***Machine:*** When setting up Gold's distributed feature, be sure to use well-maintained, dedicated machines, with optimal CPU and RAM.
- ***Software:*** Gold machines should only contain the software needed to run or support PhoneSweep functions (Microsoft Excel 2000 and Microsoft Word are two such programs). Turn off virus checkers, power management and screen savers. If you do need a screen saver and a screen password, try Screenlock (http://www.screenlock.com/).
- ***Security:*** Use firewalls and OS lock downs for security, remembering to test for PhoneSweep operability at each step or lock down.
- ***Power:*** Make sure your PhoneSweep Gold machine has a redundant power supply or is able to use the emergency power backup for your building, especially if the area it is located in is prone to power outages.
- ***Network:*** Network connections should not be on portions of your LAN that undergo heavy use.
- ***Network:*** Make Gold Distributed connections during periods of low Internet activity (heaviest Internet and LAN use tends to occur from around 12 noon to 6pm), or limit your time connected to just what you need to transfer information or control a sweep. Also, consider using Gold in Controller or Observer mode if Operator mode commands are not needed.
- ***International Machine Requirements:*** Purchase modems and other equipment that are geared for the local power and telecommunications standards. Most nations have their own standards, which is one reason why it is sometimes difficult for a modem produced in one nation to understand the dialtones in another nation.

Improving E-mail Notification Performance

To improve PhoneSweep Gold's e-mail performance, please keep the following items in mind:

- ***Who gets notified:*** Verify that all notification e-mail addresses are current. Make one person responsible for notifying you when required e-mail recipients or their addresses change.
- ***Avoid notification on common events:*** Verify the composition of each phone system you sweep to avoid setting e-mail notification on common events. You can do this by speaking with whoever maintains the phone system, or by performing an initial sweep without using e-mail notification.
- ***E-mail server:*** Verify that you have a stable e-mail server that is not likely to become overtaxed by other users. (We recommend that you ensure the e-mail server itself has been locked down to prevent spammers from hijacking it for their use.) If the server has multiple connections to it (redundancy), so much the better.

- ***Other:*** Follow the PhoneSweep machine, software, firewall, OS lockdown and power guidelines listed under "Improving Distributed Performance" above.

Improving Merged Reports Performance

To improve Gold Merged Reporting performance, please keep the following in mind:

- ***Create a trial Merged Report:*** Before generating production merged reports, make one as a trial run to test your machine's capabilities.

  The cumulative number of phone numbers being merged into one report can over-tax your system if you do not have enough CPU and RAM to efficiently handle the volume of information being processed. If the total phone numbers being merged is over 10,000, we recommend that you have a minimum CPU speed of 333 MHz.

- ***Check Merged Report size before printing:*** Before printing, check the size of your report to verify that your system and printer can handle it. Be prepared to wait when generating large reports on old printers.

- ***Other:*** Follow the PhoneSweep machine, software, firewall, OS lockdown and power guidelines listed under "Improving Distributed Performance" above.

Managing Multiple Connections Across Networks

The type of network that your organization has set up can greatly affect your ability to create and maintain PhoneSweep Gold's distributed connections.

Managing Remote Connections across an internal network or VPN-based WAN

In most cases, you should be able to connect to a remote copy of PhoneSweep Gold that is located on a machine within your internal Local Area Network (LAN) or your company's Virtual Private Network (VPN)–based Wide Area Network (WAN). VPNs, as normally set up, should be transparent to all users. To connect as a Remote Manager to another copy of Gold, you need to know the IP address or host name of the other copy of Gold.

In some cases, your LAN or VPN-based WAN may be set up to only allow certain types of network traffic to pass through it. If you encounter difficulties in setting up a connection, please contact your network or systems staff for further assistance.

Managing Remote Connections across the Internet

Several factors determine how to set up a connection with locations that are not part of your LAN or VPN-based WAN. Among them are firewalls and Network Address Translation (NAT) devices.

Firewalls act as a barrier to restrict certain flows of information between your internal network and the world. They normally sit between your internal network and the router that connects you to the Internet. The default port used for incoming distributed connections is 4322, configurable in the *phonesweep.ini* file as PORT-REMOTE. This must be set on all firewalls for all copies of Gold performing distributed functions.

NAT boxes, on the other hand, allow your company to use a handful of numbered IP addresses externally, while using a reserved set of IP addresses in any way it wants on the internal network. NAT boxes essentially act as translators, providing connections to the

outside world with an Internet address the NAT uses. Anyone looking at the source of that connection will only see the externally used Internet address and not the internally used address.

If your LAN uses IP addresses beginning with 10.x.x.x, that means your network uses RFC 1918 addresses, which have been reserved for special use. These reserved addresses should only be seen on your internal LAN or company WAN. (IP addresses beginning with **192.168.x.x** or **172.16.x.x** are also part of the reserved address space).

What if my local machine uses RFC 1918 address space behind a NAT and the machine I want to control is on the Internet with a normal IP address?

You should be able to connect to the remote location, so long as both your local machine and the remote machine can themselves access the Internet. If you encounter difficulty, please contact your systems or firewall staff.

Can I connect to a remote machine on a LAN behind a NAT box?

If you are unable to connect to a remote location that is behind a NAT box, you need to ask the remote network/systems administrator to configure the network to allow your connection to go through. Configuring the NAT box to enable access will depend on the type of NAT box being used. Two common methods that a NAT box might allow are:

- Network/systems administrator assigns you a specific port number to use. Anything sent to that port will be passed to the PhoneSweep Gold machine on the internal network. To address this properly you would provide the IP address followed by a colon (:) and then the port number. For example, you are given the port number 4322 to use with the NAT's IP address of 555.555.555.555.

  555.555.555.555:4322

- Network/systems administrator assigns an Internet usable IP address to the PhoneSweep Gold machine, and either the NAT will allow that IP address through, or the network/systems administrator places the PhoneSweep Gold machine outside the NAT, but still behind the corporate firewall.

Sandstorm highly recommends that if you have a remote location with a firewall, that you place any machine running PhoneSweep Gold behind the firewall.

Internet Primer

The topics in this section cover concepts concerned with computer and network communication and operation. They are covered in brief here only as a basic introduction.

If you are new to networking concepts, we recommend that you start with a good book or an FYI (For Your Information) put out by the Internet Engineering Task Force (IETF), to explain various network concepts in plain English.

You can locate many of IETF FYIs more easily at http://www.faqs.org/. Another web site of interest is http://www.freesoft.org, which has a link to the their fairly accessible "Connected: An Internet Encyclopedia" which details several Internet concepts.

Many networking subjects, including related security issues, are fairly well explained in numerous books.

What is an IP address and what is IP? IP, or Internet Protocol, is the primary protocol used to route information over the Internet. Every end point on the Internet has an IP address, drawn from a range of numbers running from 0.0.0.0 to 255.255.255.255.

Every bit of data sent to your Local Area Network or to some point on the Internet has an associated IP address. Local Area Networks sometimes have their own versions of the Internet Protocol, such as Nortel's IPX, which are translated to IP when sent to the larger Internet.

What is RFC 1918 or Reserved Address Space? Certain IP addresses are reserved for special use (e.g. no one can use them as part of a regular Internet connection). They can be used only on an internal network. RFC 1918 gives a complete list of reserved IP addresses.

Typically, reserved address space using 10.x.x.x is used across WANs and LANs behind a NAT box. Addresses in the 10.x.x.x address space should not be seen on the Internet at large.

What exactly is Network Address Translation (NAT)? Network Address Translation (NAT) allows corporations to present a single IP address to the Internet at large, while internally using multiple IP addresses drawn from a set of IP addresses reserved for such purposes. These reserved IP addresses will be in the form of 10.x.x.x. (Sometimes called RFC 1918 addresses). You will also see them used over Wide Area Networks, particularly if you are using VPNs.

The NAT gateway tracks information about each connection in a tracking table.

What is the Internet Engineering Task Force (IETF)? The IETF, through its individual, volunteer-based workgroups, is one of the main bodies which contribute to developing and maintaining the engineering architecture, communication and security protocols or standards used on the Internet and its technologies. (http://ietf.org/). Membership is open to all.

What is a Request For Comments (RFC)? RFCs are the documents that detail the technical (engineering) and security standards of the Internet. Further information can be found at http://www.rfc-editor.org/. A complete list of Internet RFCs can also be found at http://www.faqs.org/.

What is an FYI (For Your Information)? FYIs are a subset of the IETF RFCs, which are geared for folks of all skill levels. An index of available FYIs can be found at http://www.faqs.org/rfcs/fyi/fyi-index.html. A complete list of Internet RFCs can also be found at http://www.faqs.org/.

Other networking terms:

- **SMTP** (Simple Mail Transfer Protocol): Protocol used to send out e-mail messages.
- **POP** (Post Office Protocol): A common method used to download messages from a mail server to a personal computer.

Miscellaneous Questions

I want to set up PhoneSweep Gold's distributed feature in multiple countries. What do you recommend in terms of equipment?

Remember to purchase equipment from local suppliers for each copy of PhoneSweep Gold you intend to set up. Every country has its own telecommunications standards, so modems especially must be geared for each country. Zoltrix and MultiTech modems can be purchased on a worldwide basis. Please see the main PhoneSweep manual for further information on modem recommendations, or visit our website for the most up-to-date information: http://www.sandstorm.net.

Appendix B: PhoneSweep Gold Troubleshooting Guide

This section contains a list of common problems using PhoneSweep Gold and their possible solutions, as well as explanations of warnings and error messages.

Common Problems and Possible Solutions

Distributed

- **Issues of slow throughput over the Internet circuits**

  Slow throughput between remote copies of PhoneSweep Gold can be due to any number of factors. Some may be local to either machine's operation or problems with their LANs. Others, especially depending on time of day at either site, can be due to the level of activity or problems on the Internet at large.

  However, at all points, we recommend that you begin your troubleshooting by confirming that both your local copy of PhoneSweep Gold and the remote copy of PhoneSweep Gold are working properly before turning attention to possible network issues.

- **Basic Internet Troubleshooting skills**

  Once you have ruled out computer problems with both your location and the remote location, you may wish to take a look at your local area networks and the Internet as well.

  - Certain types of traffic are dropped (simply not passed on) during periods of high Internet traffic. Tools which use SNMP, such as Ping and Traceroute, are among those affected. In most instances, you will get a response saying there is high traffic, but often, you will get network timeouts.
  - Firewalls often block SNMP-based traffic from crossing into their LAN.
  - Internet traffic flows do not take the same path. Some tools need to be tested from two or three points in order to get accurate results. This is due to the fact that many Tier 1 (nation and world-wide) Internet Service Providers (ISPs) "shape" their traffic flows, so that traffic going between two points may take different paths across their network, dependent on which direction they are going. This means that if you see "slow times" you do not know whether the problem was on the outgoing or the return path. Also, even quick times reflect how long it took the query and response to travel from you and back to you. For accurate network troubleshooting, we recommend you get information from the following points (This is why it is better that your systems administrator does this, as they can have their ISP talk to other ISPs if need be).
    - Your machine (or from the firewall)

- Remote machine (or from the edge of remote firewall)
- A third location outside both LANs, which can then test to both LANs. For best results, it should be from a location seen on one of the previous tests (or you can use a Looking Glass – a router that allows you to perform various tests from their site).

Sandstorm suggests that wherever possible, you have your own network personnel check possible throughput issues.

If you need to perform the initial checks yourself, or want to understand how these issues can be checked, the following tools can help you. However, please use these tools with CAUTION.

- **Troubleshooting Tools**

  The following tools can help you initially troubleshoot network problems. These tools are not part of PhoneSweep, but are general-use networking tools usually supplied by computer manufacturers. Use Ping and Traceroute together.

  - **Ping** – SNMP-based tool used to simply see if a remote location is "responding".
  - **Traceroute** – SNMP-based tool that traces the number of hops that use Internet Addresses. If you see a large number of hops, do not take this in itself as a problem. Traceroute only shows those machines that respond to SNMP. Your data is actually passing through scores of switches and other machines, which a Traceroute will never show.
  - **NSLookup and Dig for DNS (Domain Name System) issues** – Domain Name System is a hierarchal naming scheme used on the Internet for routers and other devices which helps tell them which directories to use when determining where to send a given piece of information and it's IP address. This is the human equivalent of an IP Address. NSLookup and Dig are two tools which are used to make DNS queries. Sometimes changes in DNS files can interfere with your ability to make connections to a given site. (Please read a good DNS book before attempting to troubleshoot DNS issues).

Merged Reports

- **Slow report generation.** This can happen on slower machines, if you create a merged report from many profiles that contain a lot of call history. The slowness comes from the database processing. If slowness is a problem, try merging fewer profiles together, or use smaller profiles that have less call history. Machines with a faster CPU will exhibit better performance (see **Section 3.1.3, Merged Reporting System Requirements**).

E-mail Notifications

- **Not receiving any e-mail notifications.** Check the **Alerts** sub-tab, and verify that you have a valid To: address and outgoing mail server. Also make sure that you have at least one alert type checked under the **Mail Alert for Events** box, and that the **Mail Alert for Events box** itself is checked. Finally, make sure you have saved your settings using the **Save** button in the toolbar.

- **Receiving too many e-mail notifications.** You may want to un-check some events on the **Alerts** sub-tab. Voice Detect events in particular can generate a lot of e-mail, depending on your phone system.

PhoneSweep Gold Error and Warning Messages

Distributed messages

- **Cannot connect to remote host. Host <name> not found.** This message appears when you have tried to connect to a host that is not operable or does not exist.
- **Could not connect to host: WSAECONNREFUSED: Connection refused. 501 Encrypted key exchange failed.** This message appears when you have tried to connect to a remote host that you are not authorized to connect to. Either your Community Name does not match that of the remote, or your dongle number is not in the remote host's Access Control List for the type of connection you are attempting.
- **Communication with the host <name> has not occurred for 3 minutes, possibly because of a network problem or lag. You may disconnect from the host or wait another timeout interval. This message box will time out after 3 minutes, defaulting to Wait.** Remote hosts send, at the very least, a locale time update at least once every 2 minutes. If there is a slow network connection or other network problem, or if the remote host shuts down abnormally, this message will appear after 3 minutes of no data received from the remote host. Options are given to disconnect or wait another 3-minute timeout interval. If no choice is made after 3 minutes, as in the case of an unattended remote scan, the message box will disappear and default to waiting.
- **Connection to the remote host <name> has been lost, possibly because of a shutdown or network problem. Deleting session.** When PhoneSweep Gold shuts down normally, it informs any remote managers that it is closing. This message appears on the remote manager's screen, and will automatically close after a period of time.
- **You are already connected to the remote host <name>. If you want to change the type of remote connection, right-click on the host name in the list for options.** This message will appear if you attempt to connect more than once to the same host, which is not currently allowed. If you want to connect at a different access level, you must change the access level for the current connection, by right clicking on the host name and then choosing the access level from the pop-up menu. Access levels you are unauthorized for, as well as the current access level, will be disabled on the pop-up menu.
- **This is not an Operator session. You cannot switch to it. Observer sessions are remote, provide no control and load quickly via secure link. Controller sessions are remote, provide minimal control and load quickly via secure link. Operator sessions are remote, provide full control and may be slow loading the current profile information via secure link.** This informational message displays if you select an Observer or Controller session on the Distributed Overview, then click the Switch button. You may only switch to Operator sessions. The message is accompanied by one of the following options:

- **Do you want to convert the selected session to an Operator session and then switch to it?** You may choose to change to the Operator access level for this session. The session will then initialize and display as an Operator session, and the Distributed Overview will automatically switch to it.
- **This node is not authorized to become an Operator on the remote host.** Your dongle number is not on the remote host's Operator access control list. In order to become an Operator for that host, your number must be added to the Operator list at the remote site.

E-mail Notification messages

- **To receive e-mail notifications, you must: Fill in the To: address field on the Options->Alerts tab, with a valid e-mail address. Fill in the Outgoing mail (SMTP) server field on the Options->Alerts tab, with a valid outgoing mail server.** This message is displayed when you have turned on E-mail notification, and either the **To: address** field or the **Outgoing mail (SMTP) server** fields on the **Alerts** sub-tab are blank. In order to receive e-mail, you must have an e-mail address to send it to, as well as an outgoing mail server. You can use the same information as your regular e-mail program, or contact your systems staff for this information.

Merged Reporting messages

- **You must select at least one profile to do a merged report. Choose profiles by clicking the Profiles... button next to the Merged box.** This message appears when you have checked the Merged Reporting feature in the **Report** dialog box, and have supplied a file name for the report, but have not chosen any profiles to merge for the report. Click on the **Profiles…** button next to the **Merged** check box, to display a list of profiles to merge.

Appendix C: Sample PhoneSweep Merged Report

The following pages include an example of a PhoneSweep merged report.

Executive Summary of PhoneSweep Scan

Profile Name:	BOSTON_OFFICE_1_AUG2001, BOSTON_OFFICE_2_AUG2001, BOSTON_OFFICE_3_AUG2001
Report Generated:	Friday, August 24 2001 13:53:06
Time of First Call:	Monday, August 06 2001 15:06:53
Time of Last Call:	Monday, August 06 2001 17:51:00
Elapsed Time During Scan:	2 hours, 45 minutes, 53 seconds
Phone Numbers Assigned to Dial:	74
Number of calls made:	176
Phone Numbers Dialed using Single Call Detect™:	74
Phone Numbers Dialed using Data-only Mode:	74
Phone Numbers Dialed using Fax-only Mode:	68
Phone Numbers Checked for Data:	74
Phone Numbers Checked for Fax:	68
Search for modems completed:	100.0%
Search for fax machines completed:	91.9%
Username/password guessing completed:	0.0%
Modems found:	22
Systems compromised:	n/a

When the report was generated, PhoneSweep was configured to scan for both fax machines and modems.

PhoneSweep was configured to only connect to modems, but not to identify or attempt to penetrate them.

There were a total of 176 simulated calls made in this profile when the report was generated.

Profile Notes:

BOSTON_OFFICE_1_AUG2001 Created Mon Aug 6 14:40:33 2001

BOSTON_OFFICE_2_AUG2001 Created Mon Aug 6 14:48:04 2001

BOSTON_OFFICE_3_AUG2001 Created Mon Aug 6 14:49:03 2001

Engineering Summary of PhoneSweep Scan

Profile Name:	BOSTON_OFFICE_1_AUG2001, BOSTON_OFFICE_2_AUG2001, BOSTON_OFFICE_3_AUG2001
Scan Started:	Monday, August 06 2001 15:06:53
Scan Stopped:	Monday, August 06 2001 15:26:00
Elapsed time:	15 minutes, 18 seconds
Report Generated:	Friday, August 24 2001 13:53:06

Introduction:

PhoneSweep is a program developed by Sandstorm Enterprises (http://www.sandstorm.net) to search for modems within a set of phone numbers. PhoneSweep attempts to identify systems attached to remote modems as well as attempting to find areas of poor security by guessing common usernames and passwords.

Some modems are of higher quality than others, and can report more information about a remote phone number. These modems can recognize remote fax machines, phones answered by human beings, or simply just when a remote number is ringing. Sandstorm Enterprises, Inc. makes available a recommended modem list, including modems known to work well with PhoneSweep.

Without a recommended modem, PhoneSweep must rely on a time-based timeout to end a connection. It will only be able to differentiate between calls to modems, busy signals, and calls that timed out. PhoneSweep will not then include a list of fax, voice, and ring timeout numbers.

PhoneSweep Terminology:

Term	Definition
Anomaly	An "anomaly" is a PhoneSweep result that is not consistent and should be investigated. For instance, if a phone number is answered once with "carrier" (answered by a modem) but later on answered by a human voice, this is an anomaly and may indicate an unauthorized modem.
Brute force password guessing	"Brute Force" username password guessing means that PhoneSweep will call a remote number, and offer one of its assigned username/password pairs.
Compromised or Penetrated	A system has been "compromised" or "penetrated" if PhoneSweep was able to guess a valid username and password for that system, or the system allowed access without a username and password.
PhoneSweep	A program developed by Sandstorm Enterprises (www.sandstorm.net) to search for modems within a set of phone numbers. PhoneSweep can attempt to identify systems attached to remote modems as well as attempting to find areas of poor security by guessing common usernames and passwords.
Scan or Sweep	A PhoneSweep "scan" or "sweep" is a series of calls to a list of assigned numbers to search for modems, and possibly identify or attempt to penetrate the attached systems.
Username/password recycling	If PhoneSweep is "recycling" usernames and passwords, then it will attempt to brute force the entire username/password list on **each** modem that it finds. If it is not recycling, it will use each username/password pair on its list only once.

Call Response States:

Call response state	Explanation
Busy	This phone number was always busy when dialed. If a busy number is later redialed and is not busy, it is listed under the other category.
Carrier	The remote phone number responded with a carrier signal; a tone signal that indicates a computer is attached to the other end. A carrier signal means that electronic data transfer between two computers is possible, which may mean that network-based security can be evaded. Numbers with "carrier" are also referred to as numbers with modems attached.
Fax	A fax machine answered the remote phone line.
Ring Timeout	If your modem can detect when a remote phone number is ringing, PhoneSweep will record calls that ring past a limit as "Ring Timeout". The ring limit varies based on the time period during which the phone number was called.
Screened	A phone number is "screened" if the first part of the number is "9911" or "911". Screening is designed to prevent accidental calls to emergency numbers in certain countries, including the United States and Canada.
Timeout	PhoneSweep has timeout settings that vary depending on the time period in which the phone number was dialed. If the remote number is not ringing (or your modem cannot detect rings), and nothing answers the phone, the call times out.
Tone	The remote phone number answered with a dial tone. "Tone" calls may indicate a number that an unauthorized person may use to make toll calls at your expense. These should be checked to make sure that they cannot be misused.
Voice	If you have a modem that can detect voice, then PhoneSweep will mark human-answered calls as "voice". Answering machines and voicemail systems will also qualify as voice.

Dialed Phone Numbers:

	Total Phone Numbers With This Result	Percent of Total Phone Numbers
Assigned to Dial	74	100.0%*
Checked for Data	74	100.0%*
Carrier	22	29.7%
Tone	4	5.4%
Busy	6	8.1%
Ring Timeout	11	14.9%
Timeout	23	31.1%
Voice	3	4.1%
Screened	0	0.0%

* As a percent of the total numbers assigned to dial, as opposed to actually dialed.

The percentages may not add to 100 percent and there may be more distinct results than assigned phone numbers. This can happen if a phone number responded in two different ways. Also, if the scan was not completed, the numbers will be less than 100 percent.

Discovered Fax Machines:

	Total Phone Numbers With This Result	Percent of Total Phone Numbers
Assigned to Dial	74	100.0%
Checked for Fax	68	91.9%
Faxes found:	10	13.5%
Screened:	0	0.0%

Discovered Modems:

	Total Phone Numbers With This Result	Percent of Phone Numbers With Carrier
Numbers with Carrier:	22	100.0%
Identified	22	100.0%
Unidentified	n/a	n/a

Penetrated Modems:

	Count of systems penetrated	Percent of total penetrated systems
Penetrated Systems	n/a	n/a
Identified	n/a	n/a
Unidentified	n/a	n/a

Percent of Brute force username/password guessing attempts completed: 0.0%

Anomalies:

555-1017 responded with carrier as well as fax: a fax/modem is hooked up to this phone number.
555-1025 responded with carrier as well as fax: a fax/modem is hooked up to this phone number.
555-1033 responded with carrier as well as fax: a fax/modem is hooked up to this phone number.
555-2003 responded with carrier as well as fax: a fax/modem is hooked up to this phone number.

Systems Penetrated by PhoneSweep:

PhoneSweep did not succeed in penetrating any systems.

Carrier Numbers Found:

The following numbers responded with a modem carrier, allowing access to that system. This means that an outside person may be able to connect to your network through these numbers.

We recommend that you compare with known modem numbers, and that all modem lines be further checked to be sure that strong security is in place. Examples of poor modem security include (but are not limited to) systems without any passwords or systems with well-known or easily guessed usernames and passwords.

555-1003	555-1005	555-1007
555-1013	555-1015	555-1017
555-1023	555-1025	555-1027
555-1033	555-2003	555-2005
555-2007	555-2013	555-2015
555-2017	555-2023	555-8703
555-8705	555-8707	555-8713
781-555-5555		

Busy Numbers Found:

The following numbers were always busy when called by PhoneSweep. They may be leased lines, or voice or data lines that happened to be busy whenever PhoneSweep checked them. We recommend these numbers be checked further to ensure that they are not unauthorized modems.

555-1009	555-1019	555-1029
555-2009	555-2019	555-8709

These always busy telephone numbers can be re-scanned by increasing the **Busy Redial** value on the **Dial** Sub-Tab. When this report was generated, **Busy Redial** was set to 5.

Tone Numbers Found:

The following numbers returned a second dial tone when called by PhoneSweep. These numbers should be closely checked to ensure that outsiders cannot make calls through an internal exchange. If these tone numbers allow long-distance or international calls, you may be a target for expensive telephone fraud.

555-1030	555-2006	555-2010
555-8701		

Fax Numbers Found:

The following numbers responded with a FAX tone when PhoneSweep scanned them. FAX machines do not represent a security risk, although FAX numbers which also responded with Carrier could be unauthorized or misconfigured fax/modems.

555-1006	555-1008	555-1017
555-1018	555-1025	555-1033
555-2001	555-2003	555-2014
555-8704		

Incomplete Scan Areas:

PhoneSweep did not complete scanning for fax machines. Of the 74 phone numbers assigned for PhoneSweep to call, only 68 (91.9%) were actually called.

Identified Systems with Modems:

555-1003 -PC Anywhere
555-1005 - PPP (MS-CHAP)
555-1007 - PPP (MS-CHAP)
555-1013 - FreeBSD (UNIX)
555-1015 - FreeBSD (UNIX)
555-1017 - FreeBSD (UNIX)
555-1023 - FreeBSD (UNIX)

555-1025 - FreeBSD (UNIX)
555-1027 - FreeBSD (UNIX)
555-1033 - FreeBSD (UNIX)
555-2003 - FreeBSD (UNIX)
555-2005 - PC Anywhere
555-2007 - FreeBSD (UNIX)
555-2013 - PPP (MS-CHAP)
555-2015 - PPP (MS-CHAP)
555-2017 - FreeBSD (UNIX)
555-2023 - FreeBSD (UNIX)
555-8703 - PPP (MS-CHAP)
555-8705 - FreeBSD (UNIX)
555-8707 - FreeBSD (UNIX)
555-8713 - FreeBSD (UNIX)
781-555-5555 - PC Anywhere

Unidentified Carrier Numbers:

PhoneSweep did not discover any modems it could not identify during this sweep.

Responses from Penetrated Systems:

No responses were received from penetrated modems during this PhoneSweep scan.

Responses From Unknown Modems:

PhoneSweep did not receive any response strings from unknown modems.

Appendix A: Responses from target modems

This section suppressed by request.

Appendix B: Phone Number Taxonomy

Number:	Result:
555-1000	TIMEOUT
555-1001	TIMEOUT
555-1002	TIMEOUT
555-1003	CARRIER - PC Anywhere
555-1004	RING_TIMEOUT
555-1005	CARRIER - PPP (MS-CHAP)
555-1006	FAX
555-1007	CARRIER -PPP (MS-CHAP)
555-1008	FAX
555-1009	BUSY
555-1010	RING_TIMEOUT
555-1011	TIMEOUT
555-1012	TIMEOUT
555-1013	CARRIER - FreeBSD (UNIX)
555-1014	RING_TIMEOUT
555-1015	CARRIER - FreeBSD (UNIX)
555-1016	TIMEOUT
555-1017	CARRIER - FreeBSD (UNIX)
555-1017	FAX
555-1018	FAX
555-1019	BUSY
555-1020	TIMEOUT
555-1021	TIMEOUT
555-1022	TIMEOUT
555-1023	CARRIER - FreeBSD (UNIX)
555-1024	TIMEOUT
555-1025	CARRIER - FreeBSD (UNIX)
555-1025	FAX
555-1026	RING_TIMEOUT
555-1027	CARRIER - FreeBSD (UNIX)
555-1028	TIMEOUT
555-1029	BUSY
555-1030	TONE
555-1031	TIMEOUT
555-1032	RING_TIMEOUT
555-1033	CARRIER - FreeBSD (UNIX)
555-1033	FAX
555-2000	RING_TIMEOUT
555-2001	FAX
555-2002	TIMEOUT
555-2003	CARRIER - FreeBSD (UNIX)
555-2003	FAX
555-2004	TIMEOUT
555-2005	CARRIER - PC Anywhere
555-2006	TONE
555-2007	CARRIER - FreeBSD (UNIX)
555-2008	TIMEOUT
555-2009	BUSY
555-2010	TONE
555-2011	RING_TIMEOUT
555-2012	TIMEOUT
555-2013	CARRIER - PPP (MS-CHAP)

555-2014	FAX
555-2014	VOICE
555-2015	CARRIER - PPP (MS-CHAP)
555-2016	TIMEOUT
555-2017	CARRIER - FreeBSD (UNIX)
555-2018	RING_TIMEOUT
555-2019	BUSY
555-2020	TIMEOUT
555-2021	TIMEOUT
555-2022	RING_TIMEOUT
555-2023	CARRIER - FreeBSD (UNIX)
555-2024	TIMEOUT
555-8700	VOICE
555-8701	TONE
555-8702	TIMEOUT
555-8703	CARRIER - PPP (MS-CHAP)
555-8704	FAX
555-8705	CARRIER - FreeBSD (UNIX)
555-8706	VOICE
555-8707	CARRIER - FreeBSD (UNIX)
555-8708	RING_TIMEOUT
555-8709	BUSY
555-8710	TIMEOUT
555-8711	TIMEOUT
555-8712	RING_TIMEOUT
555-8713	CARRIER - FreeBSD (UNIX)
781-555-5555	CARRIER - PC Anywhere

Appendix C: List of all calls and their results

Call time: Number: Result:

This section suppressed by request.